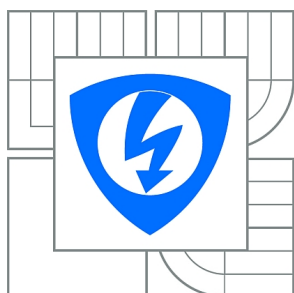




**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**  
BRNO UNIVERSITY OF TECHNOLOGY



**FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH  
TECHNOLOGIÍ**  
**ÚSTAV TELEKOMUNIKACÍ**

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION  
DEPARTMENT OF TELECOMMUNICATIONS

# MULTIMEDIÁLNÍ PŘENOSY V BEZDRÁTOVÝCH SÍTÍCH

MULTIMEDIA TRANSMISSIONS IN WIRELESS NETWORKS

**BAKALÁŘSKÁ PRÁCE**  
BACHELOR'S THESIS

**AUTOR PRÁCE**  
AUTHOR

**KAREL ZICHA**

**VEDOUCÍ PRÁCE**  
SUPERVISOR

**Ing. RADKO KRKOŠ**

BRNO 2013



**VYSOKÉ UČENÍ  
TECHNICKÉ V BRNĚ**

**Fakulta elektrotechniky  
a komunikačních technologií**

**Ústav telekomunikací**

# **Bakalářská práce**

bakalářský studijní obor  
**Teleinformatika**

**Student:** Karel Zicha

**ID:** 134443

**Ročník:** 3

**Akademický rok:** 2012/2013

**NÁZEV TÉMATU:**

## **Multimediální přenosy v bezdrátových sítích**

### **POKYNY PRO VYPRACOVÁNÍ:**

Analyzujte problematiku paketového přenosu dat bezdrátovými sítěmi se zaměřením na IEEE 802.11 WLAN. Nastudujte vliv přenosu rádiovým prostředím, sdílení přenosového média uživateli a různými sítěmi, problému skrytého uzlu a různých přístupových metod, aktuálního vytížení sítě, externího rušení a použití různých protokolů transportní vrstvy (TCP, UDP, DCCP, SCTP) na streamované přenosy a přenosy v reálném čase. Teoretický rozbor doplňte měřením ilustrujícím vliv uvedených jevů. Nastudujte možnosti QoS v bezdrátových sítích, obeznamte se s technologií qWave a přestudujte její možnosti. Zaměřte se zejména na pokročilé funkce jako měření přenosového kanálu a notifikaci aplikací o změně podmínek. Analyzujte podporu technologie qWave v domácích a průmyslových směrovačích a taky v aplikacích. Popište podporované aplikace. Prozkoumejte možnosti a limity nasazení WLAN sítí pro průmyslové sledování objektů v reálném čase. Popis doplňte měřením.

### **DOPORUČENÁ LITERATURA:**

- [1] WALKE, Bernhard H., Stefan MANGOLD a Lars BERLEMANN. IEEE 802 Wireless Systems: Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence. Reprinted March 2008. Chichester: John Wiley & Sons, 2006, xix, 382 s. ISBN 04-700-1439-3.
- [2] MORROW, Robert. Wireless network coexistence. New York: McGraw-Hill, 2004, xvii, 444 s. ISBN 00-713-9915-1.

**Termín zadání:** 11.2.2013

**Termín odevzdání:** 5.6.2013

**Vedoucí práce:** Ing. Radko Krkoš

**Konzultanti bakalářské práce:**

**prof. Ing. Kamil Vrba, CSc.**

*Předseda oborové rady*

## **ABSTRAKT**

Cílem této práce je shrnout vlastnosti bezdrátových sítí pracujících v pásmu 2,4 GHz. V první části jsou rozvedeny teoretické poznatky o architektuře sítí a porovnání jednotlivých standardů; druhy rušení způsobené externími zařízeními, mimo jiné i problematika skrytého uzlu. Jsou popsány možnosti poskytování kvality služeb v návaznosti na sadu qWave. Dále jsou zkoumány jednotlivé přístupové metody a multimediální protokoly. Druhá část je tvořena praktickým ověřením těchto poznatků. Byly provedeny testy propustnosti jednotlivých sítí v závislosti na typu problematiky. V závěru jsou tyto zaznamenané poznatky popsány a vyhodnoceny.

## **KLÍČOVÁ SLOVA**

WLAN, qWave, RTS/CTS, propustnost, skrytý uzel, QoS, standard 802.11

## **ABSTRACT**

The aim of the thesis is to summarize the qualities of wireless networks operating in the frequency band of 2.4 GHz. In the first part, theoretical knowledge about the architecture of the networks and the comparison of individual standards are presented; the types of interference caused by external devices, including the issue of a hidden node. The possibilities of providing quality services are described following the qWave set. Further, we explore individual access methods and multimedia protocols. The second part comprises the practical verification of this knowledge. The throughput tests of the individual networks were conducted regarding the type of the issue. In the conclusion, the recorded knowledge is described and evaluated.

## **KEYWORDS**

WLAN, qWave, RTS/CTS, throughput, hidden node, QoS, standard 802.11

ZICHA, K. *Multimediální přenosy v bezdrátových sítích*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. 65 s. Vedoucí práce byl Ing. Radko Krkoš

## PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Multimediální přenosy v bezdrátových sítích“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

Brno .....

.....

(podpis autora)

## Poděkování

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Radku Krkošovi za odborné vedení, konzultace a podnětné návrhy k této práci. Dále bych chtěl také poděkovat své rodině a přátelům.

# OBSAH

Úvod	12
<b>1 Standard IEEE 802.11</b>	<b>13</b>
<b>2 Modulační techniky</b>	<b>15</b>
2.1 FHSS . . . . .	15
2.2 DSSS . . . . .	15
2.3 MIMO . . . . .	16
2.4 OFDM . . . . .	16
<b>3 Architektura a druhy bezdrátových sítí</b>	<b>17</b>
<b>4 Faktory ovlivňující bezdrátové přenosy</b>	<b>19</b>
4.0.1 Rušení v bezdrátových sítích . . . . .	20
<b>5 Quality of Service</b>	<b>23</b>
5.1 Historie QoS systému Windows . . . . .	23
5.2 Důvod potřeby QoS . . . . .	23
5.3 Parametry QoS . . . . .	24
<b>6 Quality of Windows Audio/Video Experience</b>	<b>25</b>
6.1 Architektura qWave . . . . .	26
6.2 Služby na kterých je qWave závislý . . . . .	27
6.2.1 Link -Layer Topology Discovery Mapper I/O Driver . . . . .	27
6.2.2 Plánovač paketů technologie QoS . . . . .	27
6.2.3 Vzdálené volání procedur (RPC) . . . . .	28
<b>7 Řízení přístupu u standardu 802.11</b>	<b>29</b>
7.1 Metody DCF a PCF . . . . .	29
7.1.1 DCF (distribuovaná koordinační funkce) . . . . .	29
7.1.2 PCF (Centralizovaná koordinační metoda) . . . . .	30
7.1.3 Mezirámcové mezery . . . . .	30
<b>8 Standard 802.11e</b>	<b>32</b>
8.1 Uvedení do standardu . . . . .	32
8.2 HCF a EDCF . . . . .	32
8.2.1 HCF (Hybridní koordinační metoda) . . . . .	32
8.2.2 EDCF (Rozšířená DCF) . . . . .	33
8.3 WMM – Wi-Fi Multimedia . . . . .	33

8.3.1	Vlastnosti standardu WMM . . . . .	34
8.4	Vazba mezi WMM a 802.11e . . . . .	35
<b>9</b>	<b>Protokoly zajišťující přenos</b>	<b>36</b>
9.1	Transportní protokoly . . . . .	36
9.1.1	TCP protokol . . . . .	36
9.1.2	UDP protokol . . . . .	36
9.1.3	Porovnání TCP a UDP u přenosu v reálném čase . . . . .	36
9.1.4	SCTP Protokol . . . . .	37
9.1.5	DCCP Protokol . . . . .	39
<b>10</b>	<b>Přenos v reálném čase</b>	<b>40</b>
10.1	Protokoly pro multimedia . . . . .	40
10.1.1	RSVP protokol . . . . .	40
10.1.2	RTP protokol . . . . .	41
10.1.3	RTCP protokol . . . . .	41
10.1.4	RTSP protokol . . . . .	41
<b>11</b>	<b>Bezdrátový přenos s využitím technologie Wi-Fi Direct</b>	<b>42</b>
11.1	Wi-Fi Direct . . . . .	42
11.2	Miracast . . . . .	42
11.3	WiDi – Wireless Display . . . . .	43
<b>12</b>	<b>Praktická část práce</b>	<b>44</b>
12.1	Řešení problematiky skrytého uzlu . . . . .	44
12.1.1	Softwarové řešení . . . . .	45
12.1.2	Hardwarové řešení . . . . .	47
12.2	Výběr a optimalizace vhodného kanálu . . . . .	48
12.2.1	Měření vzájemného rušení jednotlivých kanálů . . . . .	48
12.3	Další druhy rušení . . . . .	52
12.3.1	Rušení mikrovlnnou troubou . . . . .	52
12.3.2	Rušení Wi-Fi technologií Bluetooth . . . . .	53
<b>13</b>	<b>Výsledky a zhodnocení práce</b>	<b>55</b>
13.1	Problematika skrytého uzlu . . . . .	55
13.2	Výběr a optimalizace vhodného kanálu . . . . .	55
13.3	Další druhy rušení . . . . .	56
<b>14</b>	<b>Závěr</b>	<b>57</b>
	<b>Literatura</b>	<b>59</b>

Seznam symbolů, veličin a zkratk	61
Seznam příloh	64
A Obsah elektronické přílohy	65



# SEZNAM OBRÁZKŮ

2.1	Princip přenosu pomocí FHSS . . . . .	15
3.1	QoS využití . . . . .	17
3.2	Režim Ad-hoc . . . . .	17
3.3	Režim Mesh . . . . .	18
3.4	Režim infranstrukturní sítě . . . . .	18
4.1	Znázornění vícecestnosti . . . . .	19
4.2	Znázornění skrytého uzlu . . . . .	21
4.3	RTS/CTS komunikace . . . . .	21
4.4	Překrývání kanálu v pásmu 2,4 GHz . . . . .	22
5.1	QoS využití . . . . .	24
6.1	qWave – zpětnovazebná smyčka . . . . .	26
6.2	qWave – závislost služeb . . . . .	27
7.1	Model soutěžení Distribuované koordinační funkce . . . . .	29
7.2	Struktura superrámce . . . . .	30
7.3	Mezirámcové mezery . . . . .	31
8.1	Fronty jednotlivých přístupových kategorií WMM klientovi [5] . . . . .	34
8.2	Časování u WMM technologie [5] . . . . .	35
9.1	Paket SCTP s hlavičkou a chunkem . . . . .	37
9.2	Porovnání navázání spojení u TCP a SCTP . . . . .	38
9.3	Popis selektivního potvrzování . . . . .	39
9.4	Popis mutli-homingu . . . . .	39
10.1	Rozdělení Deadline . . . . .	40
11.1	Sestavení relace standardu Miracast . . . . .	42
11.2	Detekování dostupných zařízení s technologií WiDi . . . . .	43
12.1	Schéma domu pro ilustraci skrytého uzlu . . . . .	44
12.2	Nastavení režimů . . . . .	45
12.3	Graf propustnosti . . . . .	46
12.4	Graf ztrátovosti . . . . .	46
12.5	Nastavení hodnoty RTS Threshold . . . . .	47
12.6	Schéma domu pro ilustraci překrývání kanálů . . . . .	48
12.7	Schéma překrývání wi-fi sítí se středovým kanálem 7 a 9 . . . . .	49
12.8	Nastavení vysílacího výkonu routeru . . . . .	50
12.9	Porovnání propustnosti při změně podmínek . . . . .	51
12.10	Bezdrátové médium v klidovém stavu . . . . .	52
12.11	Bezdrátové médium při spuštění mikrovlnné trouby . . . . .	52
12.12	Propustnost sítě při spuštění mikrovlnné trouby v programu jperf . . . . .	53
12.13	Schéma zapojení – rušení pomocí technologie Bluetooth . . . . .	54

12.14	Propustnost linky bez vnějšího rušení . . . . .	54
12.15	Propustnost rušené linky technologií Bluetooth . . . . .	54

# SEZNAM TABULEK

1.1	Charakteristika variant fyzické vrstvy podle IEEE 802.11 . . . . .	13
7.1	Hodnoty mezirámcových mezer pro jednotlivé standardy [20] . . . . .	31
8.1	Tabulka priorit Wi-fi Multimedia [5] . . . . .	34
12.1	Tabulka hodnot u režimu CTS-to-self . . . . .	45
12.2	Tabulka hodnot u smíšeného režimu . . . . .	45
12.3	Tabulka hodnot u režimu RTS/CTS . . . . .	46
12.4	Porovnání propustnosti u překrývajících se kanálů . . . . .	49
12.5	Porovnání propustnosti u překrývajících se kanálů (snížení vys. výkonu)	51

# ÚVOD

V dnešní době se stále více rozmáhají přenosy bezdrátovou sítí a požadavky na její chod se neustále zvětšují. Bezdrátová síť je charakterizována rychlou a snadnou implementací ve srovnání s metalickou sítí. Její provoz je však omezen pro běžného uživatele na bezlicenční pásma 2,4 GHz a 5 GHz. Prvně jmenované pásmo je u nás více používáno, především z důvodu nižší ceny síťových komponentů. Tato výhoda je ovšem vykoupena menším počtem vzájemně fungujících sítí a širšími možnostmi rušení od zařízení pracujících v tomto pásmu.

Tyto nežádoucí jevy mají za následek snížení propustnosti sítě nebo mohou dokonce přispívat k jejím výpadkům. Proto je důležité optimalizovat jednotlivé nastavení sítí a předejít tak situacím, které mohou nastat a omezit tak provoz na bezdrátovém médiu. Tato optimalizace je nezbytná například v bytových domech, kde máme mnoho účastníků bezdrátového provozu a bez vhodného nastavení bude síť pracovat jen ve velmi omezeném rozsahu.

V další části jsou teoreticky rozvedeny multimediální přenosy v reálném čase, které jsou velmi náchylné na zpoždění. Z těchto důvodů je nutné zajistit určitou podporu kvality přenosu.

Prostředky, které tuto službu umožňují, jsou mechanismy QoS (Quality of Service). Slouží pro rezervaci a řízení datových toků v telekomunikačních a počítačových sítích. Tato poskytnutá služba se snaží zajistit vyhrazení dostupné přenosové kapacity, aby se nesnižovala kvalita přenosu při zahlcení sítě. Pro podporu multimedií je zde popsán standard 802.11e.

Služba, která také souvisí s multimediálním přenosem je sada qWave (Quality of Audio/Video Experience), podporuje audio a video scénáře v domácích sítích a umožňuje více multimediálních proudů současně. V této práci jsou zmíněné mechanismy porovnány a jsou zde uvedeny jejich teoretické vlastnosti a možnosti.

Velká část této práce je věnována problematice skrytého uzlu. Tento jev může často nastávat ve venkovních nebo rozlehlých bezdrátových sítích, kde jsou stanice rozmístěny příliš daleko od sebe. Je zde uvedena praktická ukázka této situace a jsou znázorněny metody řešení.

Dále je provedena optimalizace výběru vhodného kanálu v závislosti na rušení od sousedních Wi-Fi sítí a měření propustnosti ovlivněné sítě. Jsou zde také změřeny a porovnány další druhy rušení pásma 2,4 GHz, tj. rušení mikrovlnnou troubou a rušení technologií Bluetooth.

# 1 STANDARD IEEE 802.11

Bezdrátové sítě WLAN byly specifikovány s cílem rozšíření technologie LAN s možností přenosu dat prostřednictvím radiových vln (RF - Radio Frequency) mezi počítači v síti se zachováním standardu se sítěmi Ethernet, Token Ring a s podporou aplikací sítě LAN. Bezdrátové sítě jsou budovány nejen na podnikové úrovni, ale i jako veřejné a domácí sítě WLAN.

Standard 802.11 byl představen v roce 1997 organizací IEEE (The Institute of Electrical and Electronics Engineers). Tento standard se začal uplatňovat tam, kde bylo z technických nebo jiných důvodů nepříliš výhodné použití optické či mechanické kabeláže. [1].

Sítě WLAN jsou charakterizovány bezdrátovým přenosem v pásmech 2,4 GHz a 5 GHz, kde je přenosové medium sdíleno jednotlivými síťovými uzly.

Tab. 1.1: Charakteristika variant fyzické vrstvy podle IEEE 802.11

Standard	Pásmo[GHz]	Přenosová rychlost[Mbit/s]	Modulace	Vydání
802.11	2,4	2	DSSS, FHSS	1997
802.11a	5	54	OFDM	1999
802.11b	2,4	11	DSSS	1999
802.11g	2,4	54	DSSS, OFDM	2009
802.11n	2,4 a 5	600	MIMO, OFDM	2008
802.11ac	5	1000	MU-MIMO	2013

## 802.11a

Standard 802.11a byl ratifikován v roce 1999 a funguje v rozsahu frekvencí 5 GHz. Z tohoto důvodu není kompatibilní s protokoly 802.11b a 802.11g, ale zároveň vylučuje rušení těmito zařízeními. Tento standard je v Evropských podmínkách přizpůsoben na 802.11h, kvůli blokaci pásma 5 GHz organizací ETSI (European Telecommunication Standards Institute.)

Další rozdíl spočívá v tom, že protokol 802.11a podporuje mezi 12 až 23 nepřekrývajícími se kanály, oproti třem nepřekrývajícím se kanálům u standardů 802.11b/g. Díky použití modulační metody OFDM se kanály mohou překrývat. Přenos datových paketů je pomalejší, ale v ohledu na chybovost je méně náchylný než rychlé pakety.

Standard 802.11a je unikátní tím, že frekvenční pásmo dělí na více částí. Tyto části označujeme jako pásma UNII (Unlicensed National Information Infrastructure), které jsou navrženy k odlišným účelům. Jednotlivé části jsou UNII 1-3. [7]

- UNII-1 je určeno pro použití v interiérech s trvalou anténou.
- UNII-2 použití v interiérech nebo exteriérech s externí anténou.
- UNII-3 slouží pro vnější mosty a externí antény.

### **802.11b**

Protokol 802.11b představuje doplněk protokolu 802.11 a také stejný počet kanálů a to 11. Používá modulační metodu DSSS, kde je signál rozprostřen celým frekvenčním spektrem. Nabízí přenosové rychlosti až 11 Mb/s. V současné době je nahrazen rychlejšími standardy. [13]

### **802.11g**

Tento protokol s maximální přenosovou rychlostí dat 54 Mb/s, se dostal na stejnou rychlostní úroveň jako protokol 802.11a, s tím rozdílem, že pracuje ve frekvenčním rozsahu 2,4 Ghz. Pro rychlosti do 11 Mb/s je kompatibilní s protokolem 802.11b a používá i stejnou modulaci. Z důvodu vyšších přenosových rychlostí používá tento standard i modulační metodu OFMD. [3]

### **802.11n**

Standard vznikl v roce 2004 a byl ustanoven organizací Wi-Fi Alliance. Cílem tohoto standardu bylo poskytnout rychlost srovnatelnou s metalickým spojením. Bylo zvažováno použít šířku kanálu 40 MHz, tím by se zvýšila i přenosová rychlost. Za těchto předpokladů by se ovšem omezil počet kanálů. Nakonec zůstaly obě varianty 20 MHz a 40 MHz. Hlavní předností standardu je využití obou pásem 2,4 GHz a 5 GHz. Dále je zde zpětná kompatibilita se staršími standardy 802.11 a/b/g. Technologie MIMO nám zaručuje větší spolehlivost, propustnost a pokrytí. [7]

### **802.11ac**

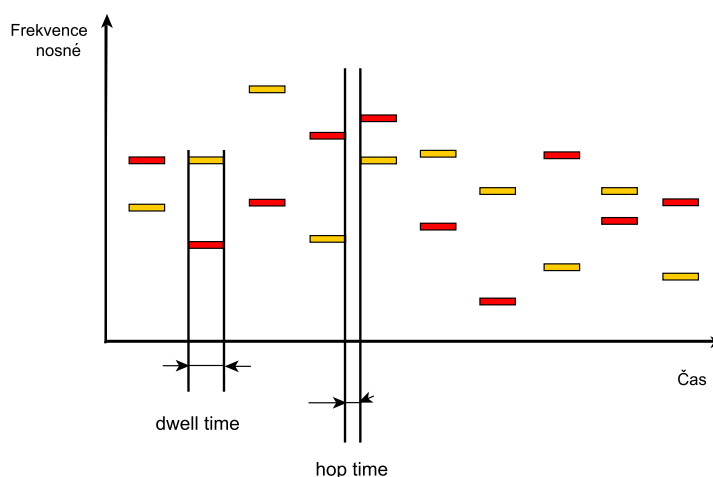
V současné době se jedná o nejnovější standard, který pracuje v kmitočtovém pásmu 5 GHz a jeho šířka pásma může být až do 160 MHz. Je zde použita multi uživatelská technologie MU-MIMO, kde jedna nebo více antén může přijímat nebo vysílat několik nezávislých datových HD streamů současně. Díky přenosovým rychlostem až 1 Gbit/s za sekundu, je tento standard vhodný pro synchronizaci a zálohování velkých datových souborů. [5]

## 2 MODULAČNÍ TECHNIKY

### 2.1 FHSS

Technologie FHSS (Frequency Hopping Spread Spektrum) pracuje v bezlicenčním pásmu 2,4 GHz – 2,485 GHz a je založena na principu, kde během přenosu není pevně nastavená nosná frekvence, ale v jednotlivých časových intervalech se mění. Tato změna frekvence je periodická.

Při použití FHSS může komunikovat více zařízení bez vlivu vzájemného rušení. Důležitou podmínkou pro fungující přenos je synchronizace vysílače a přijímače. Přenosu je charakterizován hodnotou „Dwell time“ (100 – 200 ms) a interval přeladění hodnotou „hop time“ (200 – 300 ms). Tato technologie se používá například u Bluetooth. [22]



Obr. 2.1: Princip přenosu pomocí FHSS

### 2.2 DSSS

Modulační technika DSSS (Direct Sequence Spread Spectrum) je používána pro přenos dat mezi zařízeními standardu 802.11b. Přenášený signál je rozložen napříč celým používaným spektrem. Pro kódování dat pomocí DSSS je používána čipová sekvence. Čip a bit a je v podstatě totéž, bit představuje data, zatímco čip je používán pro kódování přenosu.

Proces čipování vezme každý datový bit a rozšíří jej do podoby sekvence 11 bitů. Je zde použit tzv. Barkerův kód, který definuje použití čipů pro kódování. Dále je zde zavedena redundance – signál je rozprostřen do větší části spektra, je tedy

méně citlivý vůči rušení. Při DSSS modulaci mohou běžet maximálně 3 systémy bez vzájemného rušení. V případě, že zařízení sdílí stejný přenosový kanál nebo využívá sousední kanály těsně v jeho blízkosti, může docházet k interferenci. [7] [22]

## 2.3 MIMO

Multiple-input multiple-output (MIMO), česky více vstupů více výstupů. Je to technologie, která se využívá ve specifikaci standardu 802.11n. Tato technologie využívá několik antén pro vysílání a také pro příjem.

MIMO nabízí vysoké datové přenosy s rychlostí až 100 Mb/s na jednom kanálu díky simultánnímu multiplexingu datových proudů. Přístupové body mohou komunikovat i se zařízeními, které MIMO nepodporují, i tak dojde ke zvýšení výkonu takřka o 30 procent při použití standardu 802.11 a/b/g. [7]

## 2.4 OFDM

Metoda OFDM (Orthogonal Frequency Division Multiplex) spočívá ve využití více nosných kmitočtů s rovnoměrným odstupem. Vysílání je rozloženo do velkého počtu signálů, které nezávisle na sobě přenášejí data. Tato technika je adaptivní, protože se díky velkému počtu na sobě nezávislých signálů dokáže přizpůsobit skutečným podmínkám přenosu.

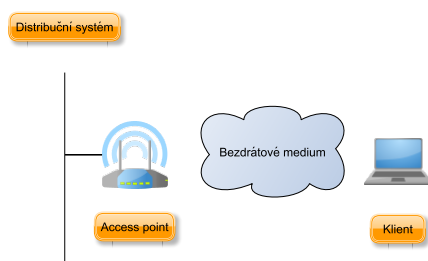
Nižší rychlosti přenosu jsou zárukou odolnosti vůči rušivým vlivům od okolního prostředí. Technologie OFDM se využívá u standardů 802.11, ADSL nebo technologie WiMAX. [7] [22]



### 3 ARCHITEKTURA A DRUHY BEZDRÁTOVÝCH SÍTÍ

#### 4 hlavní druhy fyzických komponentů

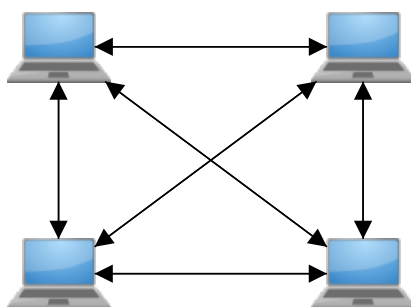
- Distribuční systém
- Přístupový bod (AP- Access Point)
- Bezdrátové médium (vzduch)
- Stanice (Station)



Obr. 3.1: QoS využití

#### Ad-hoc

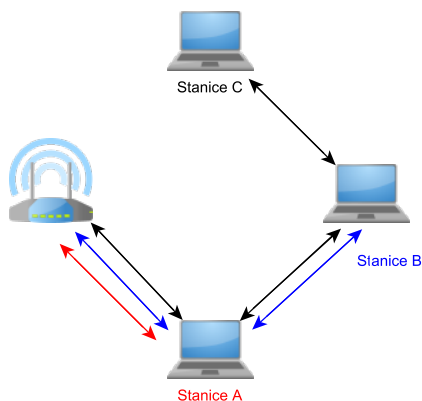
Je to typ sítě, kde stanice komunikují bez jakéhokoliv prostředníka. Sestavení sítě je přímo mezi koncovými zařízeními. Označení typu sítě je udáno značkou IBSS (Independent Basic Service Set) v beacon intervalu. Síť nemá centrální řízení a všichni klienti jsou si rovni (peer-to-peer). Další vlastností je, že stanice komunikují navzájem. Nevýhodou je však velké rušení a malá propustnost. [14]



Obr. 3.2: Režim Ad-hoc

## Mesh

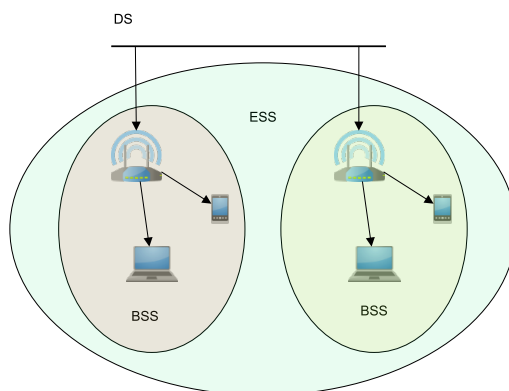
Je to zvláštní typ Ad-hoc sítí. Stanice jsou klienty a zároveň přístupovými body pro ostatní stanice v okolí. Všechny stanice jsou navzájem nahraditelné a zastupitelné. Nevýhodou Mesh architektury je využívání stanic pro komunikaci s jinými stanicemi. Dalšími vlastnostmi jsou úspora šířky pásma, zvýšený dosah sítě a nízké náklady na výstavbu. [3]



Obr. 3.3: Režim Mesh

## Infrastrukturní síť

BSS (Basic Service Set) je označení buňky, která je tvořena jedním AP a k němu připojenými stanicemi. Dále jednotlivé buňky BSS jsou sdružovány do ESS (Extended Service Set), což je skupina spolupracujících buněk. Jednotlivé AP mohou komunikovat mezi sebou prostřednictvím DS (Distribution system), může to být klasický ethernet, ale také bezdrátová technologie WDS (Wireless Distribution System). [14]



Obr. 3.4: Režim infrastrukturní sítě

## 4 FAKTORY OVLIVŇUJÍCÍ BEZDRÁTOVÉ PŘENOSY

Některé faktory mohou zkrátit vzdálenost, na kterou lze vysílat signál, nebo šíření bezdrátového signálu zcela zastavit. Mezi takové vlivy patří například absorpce, odraz, tříštění nebo vícecestnost.

### Absorpce

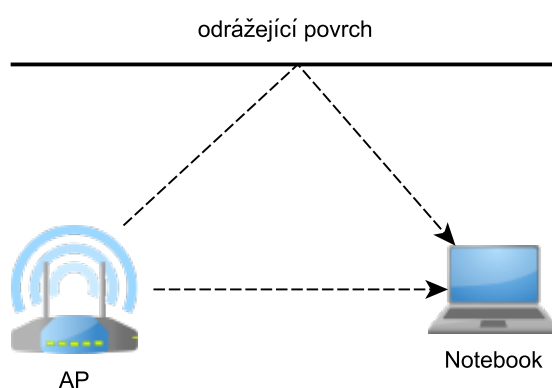
Při snižování amplitudy zmenšujeme vzdálenost, na kterou vlna putuje. Faktor ovlivňující bezdrátové přenosy při snižování amplitudy se nazývá absorpce neboli pohlcování. Není ovlivněná vlnovou délkou ani frekvencí.

Vlivem pohlcování vzniká teplo. Tento jev lze vidět například u mikrovlnných trub, které vytvářejí vlny, které jsou poté pohlcovány ohřívajícím se jídlem. Při úplném pohlcení se vlna zastaví. V bezdrátových sítích tento jev zmenšuje vzdálenost dostupnosti šíření signálu. U tohoto jevu hrají nežádoucí roli i překážky (zdi, koberce, nábytek...), které mohou signál pohlcovat. [7]

### Vícecestnost

Dochází k ní, při odrazu signálu od překážky a následném doputování signálu k cíli vícekrát. Tento jev je závislý na vlnové délce a umístění přijímače. [7]

Dalším problémem vícecestnosti je možnost dostat signál mimo fázi, v tomto případě se signály mohou navzájem vyrušit. Výsledkem bude nulový signál.



Obr. 4.1: Znázornění vícecestnosti

## Odrazy

Dalšími překážkami, které ovlivňují bezdrátové přenosy, jsou odrazy šířeného signálu. Při takovém jevu, se signál odrazí od určitého prostředí (např. zrcadlo) a šíří se jiným směrem.

Mezi takové prostředí nepatří pouze zrcadla, ale také monitory a skleněné výplně obrazů. Tento jev je závislý na frekvenci. [7]

## Rozptyl

Tento jev v bezdrátovém prostředí nastává při odesílání signálu více směry. Problém nastává při střetu s objekty s reflexním povrchem (například částice prachu ve vzduchu nebo ve vodě). Pro ukázkou této situace je ideální přestavit si paprsky světla odrážející se od rozbitého skla. [7]

Tento jev reprezentuje ve větším měřítku například i silný déšť. Vlnění prostupuje mikročásticemi dopadajících kapek a odráží se do mnoha směrů. Výsledkem je slabší signál.

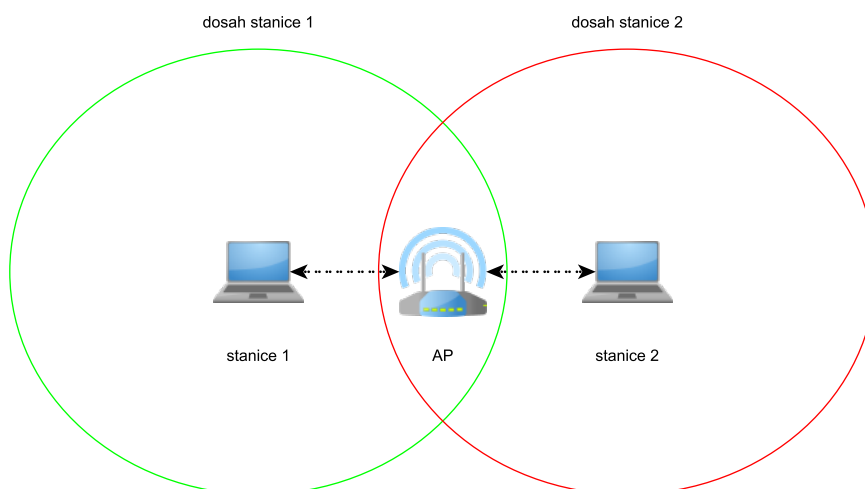
### 4.0.1 Rušení v bezdrátových sítích

Bezdrátové frekvenční pásmo 2,4 GHz je bezlicenční prostor, kde kromě Wi-Fi sítí pracuje dalších několik druhů zařízení. Tyto zařízení se mohou vzájemně ovlivňovat. Patří mezi ně například mikrovlnné trouby, bezdrátové telefony, bezdrátové herní ovladače, ZigBee a tak dále. tyto zařízení neumí komunikovat se standardem 802.11 a mohou vést k významné ztrátě propustnosti bezdrátových sítí. [21]

## Skrytý uzel

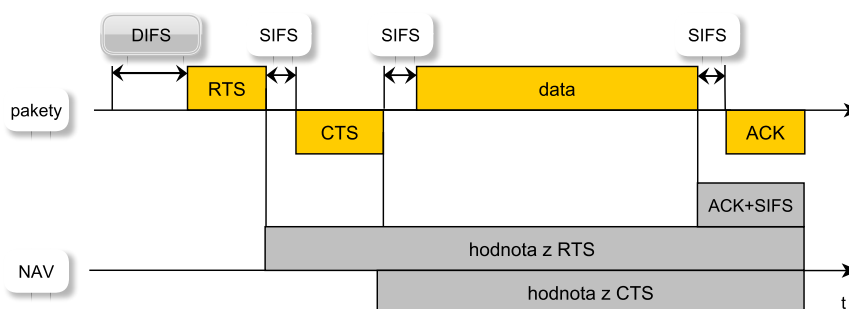
Standard 802.11 nebyl původně určen pro venkovní síť. Při jeho návrhu bylo zahrnuto nahrazení vnitřní ethernetové sítě, kde se počítalo s tím, že bezdrátové prvky náležící síti na sebe uvidí. Problém ovšem nastane, když stanice (uzly) jsou odděleny překážkou, odstíněny nebo jsou moc daleko od sebe (častý problém venkovních bezdrátových sítí).

Tyto stanice totiž nedokážou detekovat odesílání dat druhých stanic a předpokládají, že žádná další stanice právě teď nevysílá a začnou vysílat samy. Na přístupovém bodu je pak detekována kolize více stanic a data se musí znovu posílat. Tento nežádoucí stav se nazývá "problém skrytého uzlu" a má za následek snížení propustnosti a nárůst chybovosti paketů. Může značně omezit komunikaci na síti, řádově až o desítky procent. [19]



Obr. 4.2: Znázornění skrytého uzlu

Na obrázku 4.2 jsou znázorněny stanice 1 a 2, které komunikují s přístupovým bodem způsobem point-to-Multipoint. AP vidí obě stanice, protože používá všesměrové vysílání. Dále jsou zde znázorněny dosahy stanic 1 a 2, které navzájem o své komunikaci nevědí. Stanice proto mohou mylně počítat s tím, že je medium volné a tudíž mohou odesílat svá data. Pro potlačení těchto problémů se používá mechanismus RTS/CTS potvrzování. [19]



Obr. 4.3: RTS/CTS komunikace

### Funkce mechanismu RTS/CTS brání kolizím

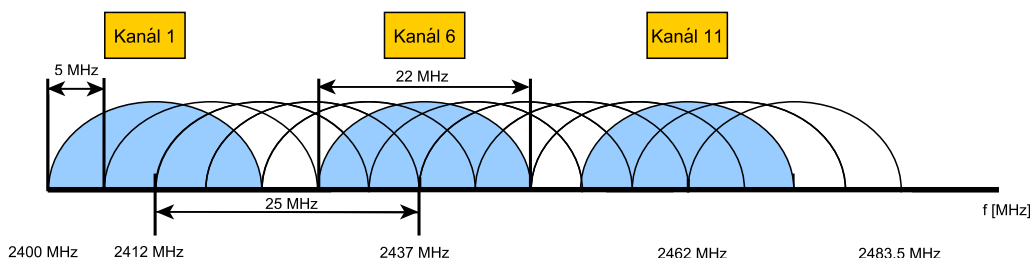
1. Stanice, která chce vysílat data, si zjistí, jestli je síť volná v časovém intervalu DIFS (Distributed Inter Frame Space)
2. Jestliže je síť v tomto intervalu stále obsazena, přenos je odložen
3. Pokud je síť volná, je vyslán krátký packet RTS (Request To Send) obsahující informace o době trvání přenosu

4. Stanice na konci spojení odpovídá (po uplynutí časového okamžiku SIFS) pakem CTS (Clear To Send), který obsahuje opět dobu trvání přenosu
5. Stanice, které obdrží RTS nebo CTS si vede tzv. NAV (Network Allocation Vector), je v něm vedena časová hodnota, po kterou je médium rezervováno. Je-li NAV nenulový, je médium považováno za obsazené, i když právě žádný signál nepřichází
6. Celý proces je při zdárném přenosu dat ukončen odesláním paketu ACK (Acknowledge)
7. V případě nepotvrzení pakem ACK, je stav vyhodnocen jako kolize a přenos je opakován znovu
8. RTS/CTS mechanismus dovede velkou měrou snížit pravděpodobnost kolize [19]

### Vzájemné rušení sousedních kanálů v pásmu 2,4 GHz

V pásmu 2,4 GHz máme v České republice k dispozici 13 kanálů, ovšem nejsou to plnohodnotné kanály. Z důvodu rozprostřeného spektra vyžaduje provoz 22 MHz a kanály mají odstup pouze 5 MHz.

Vysílání na jednom kanále tedy překrývá sousední 2 kanály z jedné strany a sousední 2 kanály ze strany druhé. Tedy vysílání na jednom plnohodnotném kanále zabírá téměř 25 MHz. Jestli vyžadujeme používat více přístupových bodů, které jsou v dosahu, ale aby se vzájemně nepřekrývaly a nerušily, máme k dispozici pouze 3 kanály, jejichž centrální kanály jsou od sebe vzdáleny 25 MHz. [14]



Obr. 4.4: Překrývání kanálu v pásmu 2,4 GHz

## 5 QUALITY OF SERVICE

### 5.1 Historie QoS systému Windows

#### Windows 2000

QoS mechanismy v operačních systémech prošly významnou změnou v několika letech z trendu vyplývajícího z náročnosti na šířku pásma aplikací. Už Windows 2000 obsahoval jednu z prvních verzí QoS a to Generic QoS (GQoS) aplikační programovací rozhraní (API) jako rámec pro QoS. GQoS Api umožňuje přístup k QoS mechanismům, které byly k dispozici jako součást síťového zásobníku včetně protokolu Resource Reservation (RSVP) pro signalizaci, rezervaci prostředků v síti a řízení provozu na 2. a 3. Vrstvě. Windows 2000 také poskytoval nástroj na správu šířky pásma Subnet Bandwidth Manager (SBM). [2]

#### Windows XP

U Windows XP byl kladen důraz především na stanovení priorit a na řízení provozu. Ačkoliv GQoS bylo nadále podporováno pro přístup ke QoS, rezervační mechanismy byly odstraněny. Jádrem implementujícím priority a řízení provozu se stal QoS Packet Scheduler (Psched.sys), který je přístupný přes GQoS API a aplikační rozhraní s názvem Traffic Control (TC) API, které vyžaduje oprávnění správce. QoS mechanismy stanovené v systému Windows XP poskytují podporu ve firemních pevných sítích. [2]

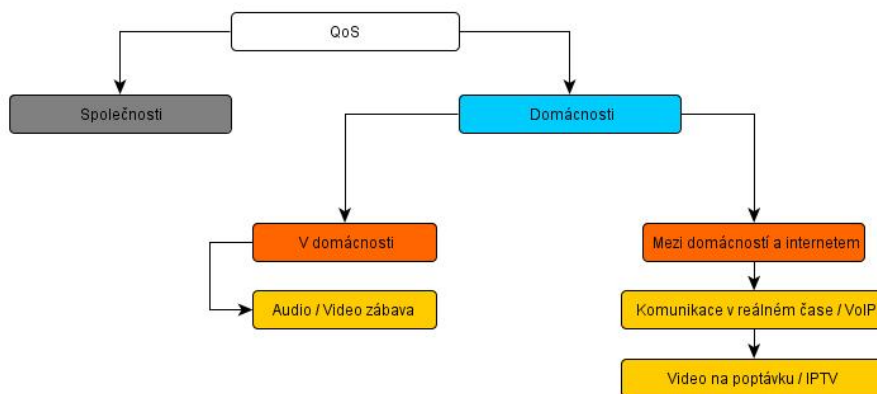
#### Windows Vista a vyšší verze

U systému Windows Vista, jsou nadále podporovány tyto QoS mechanismy a jsou rozšířeny o služby pro běžné spotřebitele a domácnosti z důvodu stále většího počtu domácích sítí a nároků na jejich provoz, tj. audio a video služby. Z toho důvodu byla zavedena služba qWave, která bude poskytovat tuto podporu pro domácí použití. [4]

### 5.2 Důvod potřeby QoS

Tradiční Wi-Fi poskytuje rovný přístup ke všem připojovaným zařízením. Když při provozu je překročena dostupná šířka pásma, propustnost pro všechny datové proudy je podobně snížena bez ohledu na typ dat. Vliv na uživatelský komfort je silně ovlivněn typem dat a druhem aplikace.

Zpoždění jedné sekundy při odesílání tiskové úlohy z počítače do tiskárny neovlivní uživatele natolik, jako například stejné zpoždění u VoIP hovoru nebo streamu, které může mít za následek špatnou kvalitu hovoru resp. zmrazení obrazu. [2]



Obr. 5.1: QoS využití

## 5.3 Parametry QoS

Hlavními parametry QoS, které ovlivňují výslednou kvalitu služeb:

### Zpoždění (Delay)

- Globální zpoždění – celková doba zpoždění při přenosu jednoho paketu
- Lokální zpoždění – časový interval na zpracování dat

### Propustnost (Throughput)

- Maximální velikost paketu
- Maximální počet datových jednotek přenesených za časový interval (paket/s)
- Maximální velikost burstu

### Ztrátovost (Loss rate)

- Loss rate – maximální počet ztrát za jeden časový interval
- Loss size – maximální počet po sobě ztracených paketů

### Kolísání zpoždění (Jitter)

- Maximální povolená časová odchylka dat doručených do cíle. Vzniká hlavně kvůli rozdílu v délkách front v souvislosti se zahlcením sítě. Především hlasové služby jsou velice náchylné na kolísání zpoždění z důvodu vysílat a přijímat každých 20 ms. [8]



## 6 QUALITY OF WINDOWS AUDIO/VIDEO EXPERIENCE

QWave je sada kvality služeb (QoS) pro časově závislé multimediální data. Je použita v zařízeních v domácí bezdrátové síti. QWave používá inteligentní prioritizaci posílání paketu, aby zajistila co nejmenší zpoždění a zároveň zajistila vysokou kvalitu při přenosu v reálném čase.

Sada podporuje více současných multimédií. Qwave je určeno výhradně pro použití v domácích bezdrátových sítích a je zakázána v jiných prostředích, jako jsou například podnikové sítě. S ohledem na nestabilitu šířky pásma, kterou přináší bezdrátová síť, qWave používá zpětnovazebnou smyčku (viz. obr 4.1) a průběžně tak monitoruje dostupnou šířku pásma. [2]

- Pokud je mediální aplikace připravena vysílat, vyžádá si přístup od qWave, kde síťová sonda určí (použití QoS, měření experimenty), jestli je k dispozici dostatečná šířka pásma pro spuštění nového vysílání.
- qWave monitoruje síťové podmínky. Pokud se zjistí přetížení sítě (například v důsledku poklesu šířky pásma), pak informuje aplikaci.
- Pokud qWave zjistí zlepšení podmínek, oznámí to aplikaci a ta může začít vysílat data vyšší přenosovou rychlostí.

qWave nespolehá na rezervační techniky, jako jsou RSVP pro domácí stream, protože záruka rezervace pásma je bezvýznamná, jestliže Wi-Fi stanice se pohybuje od AP (přístupový bod) nebo vzniká pokles šířky pásma rušením.

Qwave poskytuje i dobrou podporu starším zařízením nebo také mobilním zařízením, která slouží pouze jako vizualizační zařízení a ne jako zdroj A/V provozu. [2]

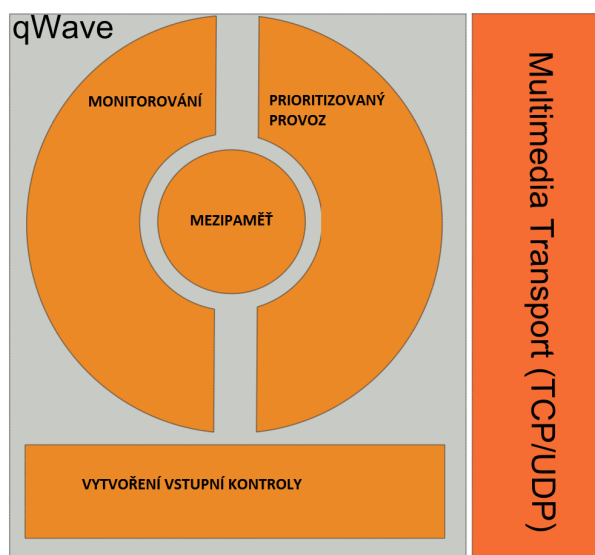
Viz příloha je zobrazena ukázka využití qWave u přenosu videa prostřednictvím domácí bezdrátové sítě při konstantní šířce pásma. Při vytěžování sítě a následném poklesu šířky pásma nevznikalo zpoždění a obraz byl plynulý. Šlo však zřetelně poznat snížení datového toku ve srovnání s ideálním stavem.

## 6.1 Architektura qWave

Architektura qWave se skládá z následujících částí:

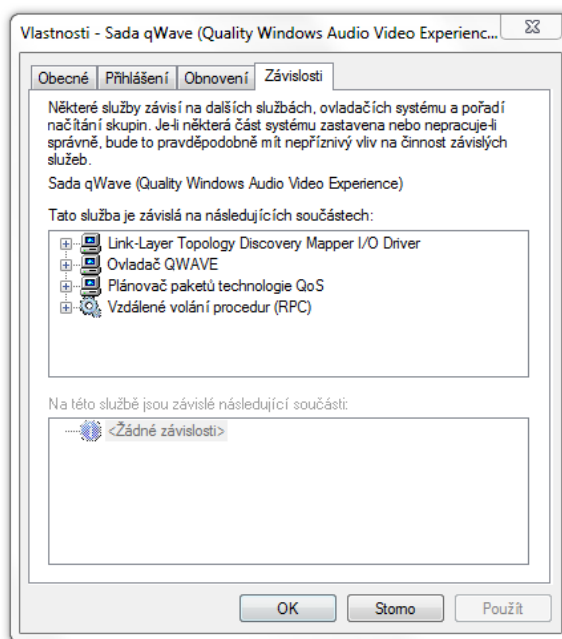
- Vstupní ovládání
- Vyrovnávací paměť
- Sledování a snímání
- Řízení provozu a označování

Vstupního ovládání zpřístupní rozhraní API používané aplikacemi k vyvolání qWave služby. Ta dále komunikuje s rozhraním transportních protokolů Real-time protokol (RTP) a Real-time Control Protokol (RTCP). [2]



Obr. 6.1: qWave – zpětnovazebná smyčka

## 6.2 Služby na kterých je qWave závislý



Obr. 6.2: qWave – závislost služeb

### 6.2.1 Link -Layer Topology Discovery Mapper I/O Driver

LLTD je vlastní protokol linkové vrstvy pro diagnostiku sítě a kvality služeb. Tento protokol pracuje na kabelové (IEEE 802.3) i bezdrátové síti (IEEE 802.11). Tento protokol je součástí Windows Vista a vyšších verzí. Jeho funkce se používá pro grafické znázornění v místní síti LAN nebo WLAN, ke které je počítač připojen. Windows XP neobsahuje protokol LLTD jako standardní součást. Počítač s tímto operačním systémem se nezobrazí na mapě sítě, pokud LLTD není doinstalován. Aktualizace Service Pack 2 a Service Pack 3 tento protokol již obsahují.

LLTD se skládá ze dvou částí. První složkou je LLTD mapper I/O je master modul, který řídí proces zjišťování a generuje mapu sítě. Příslušná oprávnění mohou být nakonfigurována s nastavením zásad skupiny. Druhou složkou jsou LLTD respondenti, kteří odpovídají na žádost mapovače na jejich hostitele a případně na další informace o síti. [10]

### 6.2.2 Plánovač paketů technologie QoS

Je to komponent, který je implementovaný v platformě Windows od verze XP a dále u vyšších modelů. Tento plánovač je určen k ovládání IP provozu pro různé síťové

služby, včetně reálného provozu v čase. Tato funkce na úrovni síťového protokolu, který rozděluje šířku pásma konkurenčním připojením.

Vysílací zařízení určuje, kolik paketů je předáno k dalšímu spojení (každý tok) v daném čase. Plánovač paketů dělá svá ustanovení pozorováním paket. Vyplývá z aplikací nebo na vyžádání od kvality služby (QoS), protokolu jako RSVP nebo DiffServ. [10]

### **6.2.3 Vzdálené volání procedur (RPC)**

Je to protokol, který může požádat program o službu, která se nachází v jiném počítači v síti, aniž by musel znát detaily sítě. Volání procedur je také někdy označováno jako volání funkce nebo volání podprogramu.

RPC používá model klient/server. Program, který výkon požaduje je klient a servis, který poskytuje program je server. RPC je synchronní operace, to znamená, že žádaný program je pozastaven do doby, než budou výsledky ze vzdálené operace doručeny. Avšak při jednoduchých procesech, které sdílí stejný adresní prostor, RPC umožňuje provedení současně. Výhodou je odlehčení vlastním aplikacím od komplikovaných procedur a možnost použít výkon vzdálených serveru.

RPC protokol pracuje na relační vrstvě referenčního modelu ISO/OSI. Mezi alternativní metody pro klient/server patří Message Queuing a IBM APPC (Advanced program – to – program communication). [10]

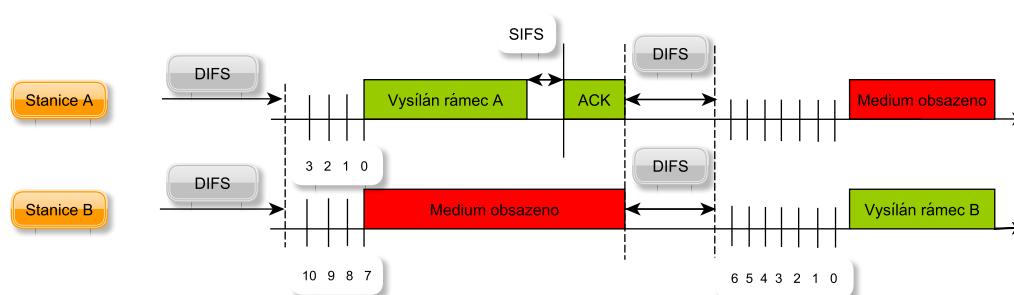
## 7 ŘÍZENÍ PŘÍSTUPU U STANDARDU 802.11

### 7.1 Metody DCF a PCF

#### 7.1.1 DCF (distribuovaná koordinační funkce)

Je to základní přístupová metoda, umožňující sdílení média technologií CSMA/CA. Stanice sleduje přenosové médium.

Pokud po uplynutí časového intervalu DIFS (Distributed Interframe Space) je přenosové médium volné, stanice pošle paket. V případě, že je médium využíváno, přenos je odsunut a stanice nadále kontroluje dostupnost média. Posílání rámců pomocí této metody má nejnižší prioritu. [3]



Obr. 7.1: Model soutěžení Distribuované koordinační funkce

#### Průběh komunikace

1. stanice čeká na vypršení intervalu DIFS
2. po uplynutí doby DIFS si stanice vygeneruje náhodné číslo
3. dále vygenerované číslo snižuje hodinovým impulzem a uplynutí této doby zkontroluje obsazenost média
4. pokud je médium volné, tak začne vysílat
5. ostatní stanice zjistí, že médium už není volné a přestanou s odpočítáváním
6. pokud byl datový rámeček přenesen úspěšně, cílová stanice čeká po dobu intervalu SIFS a poté pošle zpět potvrzovací rámeček ACK
7. po přijetí zprávy ACK je přenos ukončen [22]

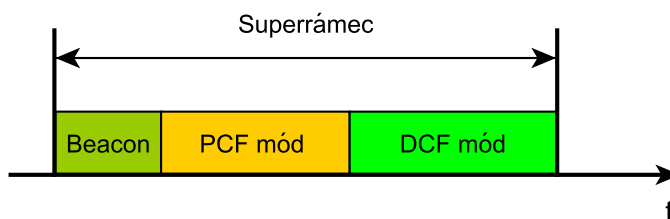
#### Vlastnosti metody DCF:

- Nepodporuje QoS
- U velkého počtu stanic větší riziko kolizí

### 7.1.2 PCF (Centralizovaná koordinační metoda)

Představuje přístupovou metodu bez soutěžení. Přístupový bod (AP) se pravidelně dotazuje všech stanic, jestli nemají data k vysílání.

Při použití této metody se definuje časový interval označovaný jako superrámec. (viz. Obr 7.2) Tato metoda se vždy používá v kombinaci s DCF. Superrámec obsahuje beacon, interval bez soutěžení (Contention-Free Period – CFP, přístupová metoda PCF) a interval soutěžící (Contention Period CP, přístupová metoda DCF).



Obr. 7.2: Struktura superrámce

Před zahájením komunikace je nutno nastavit u AP podporu PCF. Dále klient oznámí svůj záměr přístupovému bodu využívat PCF. Po vymezenou dobu se přístupový bod dotazuje stanic, jestli mají data k odeslání.

V tom případě je pošle přístupovému bodu jako odpověď na dotaz. V opačném případě je poslán prázdný rámec. Po vypršení časového úseku vymezeného pro interval bez soutěže je zahájen interval soutěžící, kde registrované stanice soutěží o přístup k médiu. [22]

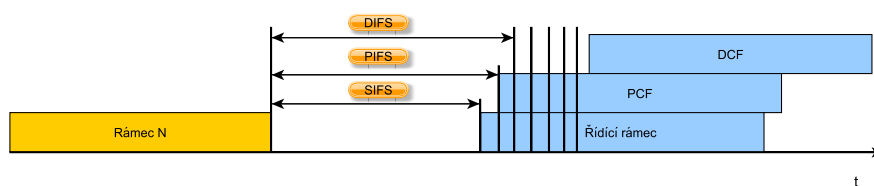
#### Vlastnosti metody PCF:

- Podpora QoS
- Vyžaduje přítomnost AP
- Malá podpora u WLAN zařízení

### 7.1.3 Mezirámcové mezery

- SIFS - je to nejkratší mezirámcová mezera, která má největší prioritu. Zajišťuje největší pravděpodobnost přístupu k médiu. Může být před nebo za rámci RTS/CTS.
- PIFS - středně dlouhá mezera. Vyšší priorita než rámce. Používá se pouze při metodě PCF

- DIFS - je základem funkce DCF. Každá stanice čeká po hodnotu DIFS a poté nastává soutěžení CP - Contention Period)



Obr. 7.3: Mezirámcové mezery

Po skončení časového intervalu DIFS je stanicí vytvořeno náhodné číslo, které je poté vynásobeno hodnotou slot time. Tato výsledná hodnota stanici určí, jakou dobu má čekat.

Tab. 7.1: Hodnoty mezirámcových mezer pro jednotlivé standardy [20]

Standard	SIFS [ $\mu$ ]	PIFS [ $\mu$ ]	DIFS [ $\mu$ ]	slot time [ $\mu$ ]
802.11a	16	25	34	9
802.11b	10	30	50	20
802.11g	10	30	50	20
802.11n	10	20	50	9

## 8 STANDARD 802.11E

### 8.1 Uvedení do standardu

IEEE je Wi-Fi doplněk standardu IEEE 802.11, vylepšující takzvanou Media Access Control (MAC) podvrstvu linkové vrstvy rozšiřující podporu kvality služeb (QoS). Standard je velice důležitý pro aplikace citlivé na zpoždění jako VoIP a streamové multimédia.

Bezdrátové sítě jsou v porovnání s metalickými méně spolehlivé a bývají nepředvídatelné. Vzniká zde problém rušení, který je způsobený podmínkami prostředí. Vzduch jako bezdrátový nosič je obtížnější na řízení sítě než metalické spojení. Bezdrátové sítě jsou dále limitovány omezenou šířkou pásma a velkými náklady na režii.

Z těchto důvodů byla do standardu 802.11e zavedena kvalita služeb QoS (Quality of Service), která se snaží splňovat požadavky aplikací a řízení datových toků. QoS využívá mechanismy kontrolující přístupy bezdrátového média. Nejdůležitější požadavky na provoz jsou šířka pásma, velikost latence a chybovost paketů.

Základní standard 802.11 nedokázal definovat prioritizace ani rozdíly mezi jednotlivými přenosy. Z těchto důvodů by síť velice neefektivní a pro náročné přenosy videa nebo hlasu nevyhovovala. Z těchto důvodů vznikl standard 802.11e, který obsahoval QoS. Tento standard zaručoval nižší režii a efektivní využití šířky pásma. V MAC vrstvě vznikly dva režimy přístupu k médiu EDCF a HCF. [6]

### 8.2 HCF a EDCF

Obě tyto metodou jsou hybridní, to znamená, že není nutno mít v síti centrální počítač, ale je vyžadován centralizovaný hybridní kontrolér. Metody vznikly za účelem poskytnutí požadovaného výkonu datového toku.

#### 8.2.1 HCF (Hybridní koordinační metoda)

Tato metoda vychází z centralizované koordinační funkce PCF. Řízení přístupu řeší hybridní koordinátor HC. Oproti EDCF, kde je přístup k médiu řízen na základě relativních priorit, HCF zaručuje absolutní garanci doby přenosu a zpoždění. Tento mechanismus podporuje jak interval bez soutěžení, tak interval soutěžení.

Společně tvoří superrámec ohraničený beacon rámci. Důležitým kritériem je konkrétní specifikace požadavků od stanic. Tyto požadavky jsou poté vyhodnoceny hybridním koordinátorem. [3] [22]



### Výhody proti metodě PCF:

- Možnost zasílání více paketu najednou
- Definice tříd provozu (Traffic Classes)
- Propracovanější zajištění QoS
- Poskytnutí informací o délce front

### 8.2.2 EDCF (Rozšířená DCF)

Metoda DCF poskytuje rovnocenný přístup všem soutěžícím stanicím. EDCF metoda vznikla jako nadstavba DCF a rozděluje provoz do osmi kategorií.

Každá stanice může mít až 4 kategorie přístupu a svůj provoz může dělit až do osmi prioritních úrovní. Aby soutěžení mezi přístupovými kategoriemi fungovalo, je zavedena další mezirámcová mezera výběru AIFS (Arbitration Interframe Space).

Podle standardu 802.11e má každá kategorie vlastní mezirámcovou mezeru, která se může variabilně nastavovat podle potřeby. Přenosy s vyšší prioritou mají kratší mezery AIFS kvůli snadnějšímu přístupu k médiu. [23]

## 8.3 WMM – Wi-Fi Multimedia

Aplikace bez podpory QoS běžící na různých zařízeních mají stejnou příležitost k přenosu datových paketů. Tento scénář dobře funguje například pro webové prohlížeče nebo přenosy souborů, ale není dostatečný pro multimediální aplikace, které jsou velmi citlivé na zpoždění přenosu nebo snížení propustnosti a vyžadují podporu kvality služeb. Mezi takové aplikace patří streamování videa a interaktivní hry. Z důvodu této potřeby byla v roce 1999 vyvinuta certifikace WMM neziskovou organizací Wi-Fi Alliance .

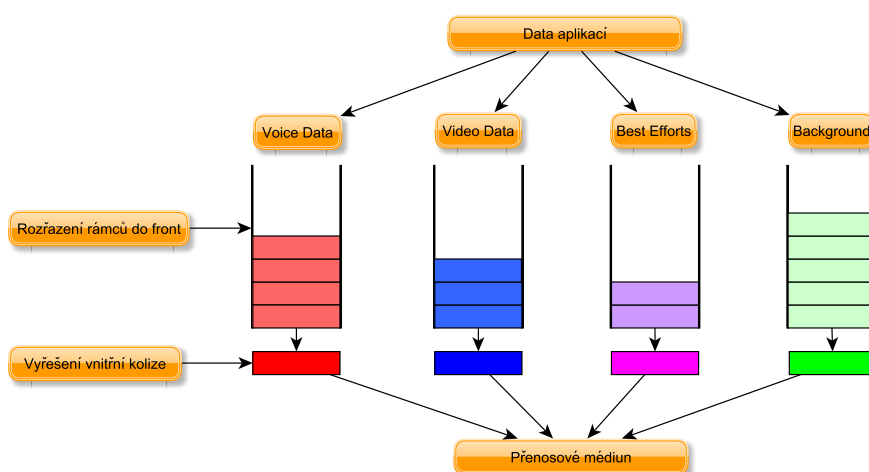
WMM přidává Wi-Fi sítím prioritizovanou QoS schopnost, která optimalizuje výkon při více navazujících aplikacích, z nichž každá má různé požadavky a zpoždění. Bezdrátové sítě bez podpory WMM nemohou poskytovat žádné priority pro datové přenosy, které jsou citlivé na zpoždění, například audio nebo video. WMM rozděluje 4 přístupové kategorie odvozené ze standardu 802.11D, které odpovídá prioritní tabulka. Tyto priority byly navrženy s konkrétními druhy dopravy, ovšem uživatel si je může přizpůsobit podle sebe a rozhodnout, která kategorie přístupu bude mít přednost, pomocí podpory QoS klienta. [5]

Tab. 8.1: Tabulka priorit Wi-fi Multimedia [5]

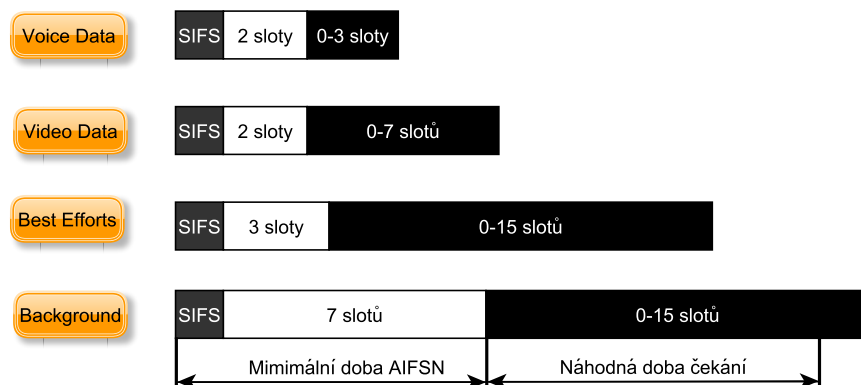
Kategorie přístupu	Popis priorit	Priority 802.1d
Priorita hlasu	Nejvyšší priorita: umožňuje více souběžných VoIP hovorů, nízké zpoždění a vysokou kvalitu zvuku	7,6
Priorita videa	Upřednostnění přenosu videa nad ostatními datovými přenosy. V sítích 802.11g a 802.11a podporuje 3-4 SDTV streamy nebo jeden HDTV stream	5,4
Priorita Best Effort	Přenos ze starších zařízení nebo aplikací, které nemají QoS a nejsou citlivé na zpoždění. Například prohlížení internetu	0,3
Priority na pozadí	Nízká priorita: stahování dokumentů, tisk, přenosy, které nemají striktní požadavky na zpoždění a propustnost	2,1

### 8.3.1 Vlastnosti standardu WMM

U bezdrátových sítí tvoří standard WMM nové mechanismy pro vrstvu MAC a to především mechanismus DCF, který je vybaven technikou předcházení kolize CSMA/CA. Tato metoda umožňuje vysílání všem zařízením současně, do doby přetížení sítě, z důvodu vysokých požadavků. Poté nastane výrazné snížení rychlosti přenosu. Stejně jako 802.11e, i WMM je založeno na čtyřech kategoriích, s tím rozdílem, že WMM je zaměřené na multimediální přenosy. [5]



Obr. 8.1: Fronty jednotlivých přístupových kategorií WMM klientovi [5]



Obr. 8.2: Časování u WMM technologie [5]

## 8.4 Vazba mezi WMM a 802.11e

Standard WMM navazuje na 802.11e s rozdílem specifikace služeb zaměřené především na multimédia a využívající podporu QoS. Je zde důležité, aby WMM bylo plně kompatibilní se standardem 802.11e.

## 9 PROTOKOLY ZAJIŠŤUJÍCÍ PŘENOS

### 9.1 Transportní protokoly

#### 9.1.1 TCP protokol

V rámci hierarchického modelu se tento protokol nachází v transportní vrstvě, nad vrstvou síťovou, se kterou sdílí protokol IP. TCP je spojově orientovanou službou přenosu, která probíhá ve 3 fázích:

- Navázání spojení
- Vlastní přenos dat
- Rozpad spojení

Tento transportní protokol nám zabezpečuje spolehlivý přenos dat a příchozí bytový tok rozděluje na segmenty. Přenos je plně duplexní, což znamená současný obousměrný provoz. TCP je využíváno aplikacemi, které vyžadují spolehlivý přenos dat (např. FTP, TELNET).

#### 9.1.2 UDP protokol

User Datagram Protokol, přenáší data prostřednictvím datagramu. Je to transportní protokol, který poskytuje nespolehlivou a nespojitou službu spojení.

Díky těmto vlastnostem má menší režii než protokol TCP. Problémy se spolehlivostí přenosu zde přebírají aplikační protokoly. UDP neposkytuje žádné záruky doručení zpráv. Protokol pouze přidává kontrolní součty a schopnost roztrždit pakety mezi více aplikací běžících na jednom počítači. [3]

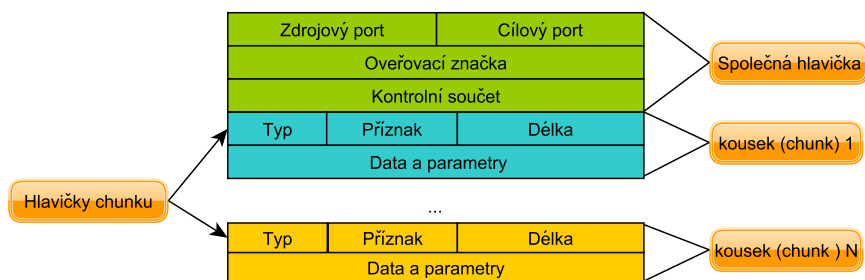
#### 9.1.3 Porovnání TCP a UDP u přenosu v reálném čase

Při přenosu hraje velkou roli ztrátovost paketů. Může nastat z důvodu zahlcení směrovačů a ten potom musí v jednom okamžiku poslat obrovské množství příchozích paketů. U aplikací přenášených pomocí protokolu TCP dojde při ztrátě paketu k jejich opětovnému poslání a tím vzniká zpoždění.

Toto zpoždění má ovšem velký vliv na aplikace v reálném čase. Z tohoto důvodu je použit nespolehlivý protokol UDP, který nepodporuje opětovné posílání paketů. Multimediální aplikace v reálném čase tolerují určitou ztrátovost paketů a to u audia i videa. [8]

### 9.1.4 SCTP Protokol

Protokol SCTP vychází z protokolů TCP a UDP. Je to spojově orientovaný protokol, který podporuje adresaci na transportní vrstvě pomocí čísel portů. Před přenosem dat je navázána komunikace a při skončení je rozpojena. Příchozí data jsou od příjemce potvrzována, takže jej můžeme považovat za protokol s bezpečným doručováním. [12]



Obr. 9.1: Paket SCTP s hlavičkou a chunkem

Společná hlavička má velikost 12 bytů. Obsahuje zdrojový a cílový port, ověření totožnosti a kontrolní součet. SCTP paket obsahuje také 32-bitový kontrolní součet. Pokud není kontrolní součet platný, je paket zahozen.

#### Kousek (chunk)

Datová část je rozdělena na jednotlivé kousky (chunky), které jsou na sobě zcela nezávislé. Každý jednotlivý chunk obsahuje svou vlastní hlavičku, která se skládá z typu, příznaku a délky chunku. Pro běžné použití je definováno 13 druhů chunku. [12]

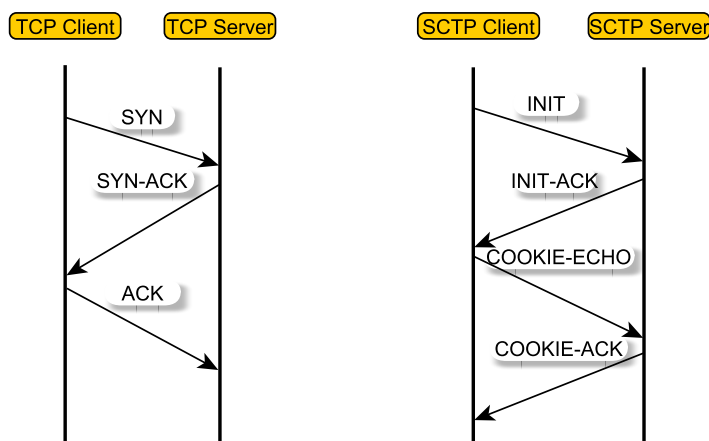
Výhody SCTP protokolu:

- Bezpečná inicializace a společné ukončení
- Selektivní potvrzování
- Multi-streaming
- Multi-homing
- One-to-one, one-to-many
- Zasílání zpráv

## Navazování spojení

Server se nachází ve stavu CLOSED. Přijímá požadavek INIT pro navázání asociace s Clientem. Z přijatých dat z INIT vygeneruje potřebné hodnoty a zašifruje je bezpečnostním klíčem. Tyto hodnoty tvoří COOKIE. Hodnoty jsou dále přeposlány zpět Clientovi ve formě INIT-ACK.

Client po přijetí ACT-INIT odesílá COOKIE-ECHO, které v sobě obsahuje strukturu COOKIE. Server ověří původce COOKIE. Při ověření, že se jedná o COOKIE vytvořené v minulosti tímto serverem, pošle Server Clientovi potvrzení COOKIE-ACK a vstoupí do režimu ESTABLISHED. V tomto režimu je Server schopen přijímat i odesílat data. [12]



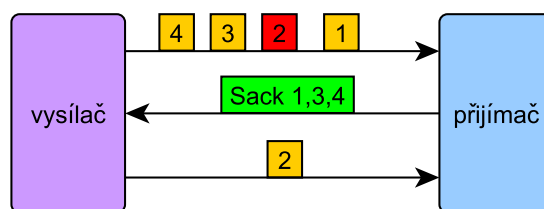
Obr. 9.2: Porovnání navázání spojení u TCP a SCTP

## Multi-streaming

Principiálně jde o oddělené vysílání více streamů v rámci jedné asociace. Teoreticky může být streamů až 65535. Z důvodu velké režie se reálné hodnoty pohybují kolem čísla 10. Jednotlivé chunky v packetu mohou obsahovat na sobě nezávislé streamy. Při vzniku chyby u streamu není ovlivněn další stream.

## Selektivní potvrzování

Velkou výhodou protokolu SCTP je selektivní potvrzování. Při posílání dat se potvrzují chunky došlé a ztracené, proto vysílací strana pošle znovu jen opravdu chybějící chunky. Díky tomuto postupu nedochází k zahlcení vysílání a ke zvětšování zpoždění. V porovnání s TCP, kde se znovu odesílají všechny pakety od doby ztráty chunku. Kontrolní chunk se nazývá SACK. [12]

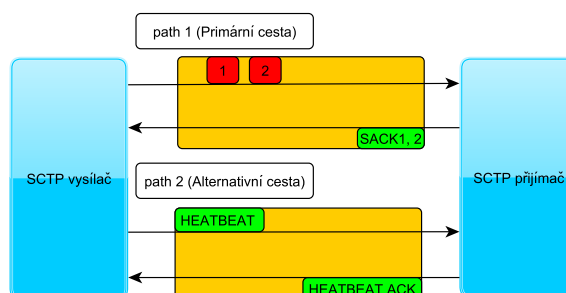


Obr. 9.3: Popis selektivního potvrzování

## Multi-homing

Je to vlastnost protokolu SCTP, která dokáže vytvořit spojení vázané na více síťových rozhraních (např. Ethernet, 802.11). Implicitně jsou data posílána po primárních cestách (Primary Address).

Pokud aktivní cesta obsahuje velký počet chyb, který přesáhne určitou hranici, SCTP implementace oznámí vyšší vrstvě nemožnost posílání dat touto cestou a data mohou být posílána alternativní cestou. Použitelná síťová rozhraní jsou posílána příjemající straně. Alternativní cesty zjistíme pomocí zprávy HEARTBEAT. Přijímající strana poté odpovídá zprávou HEARTBEAT ACK. [12]



Obr. 9.4: Popis mutli-homingu

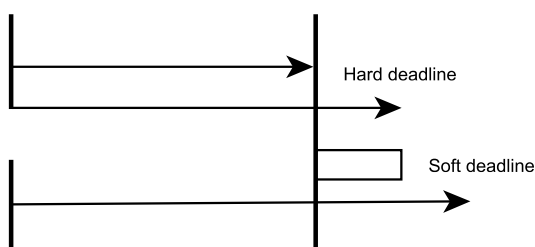
### 9.1.5 DCCP Protokol

DCCP (Datagram Congestion Control Protocol) je to datagramový transportní protokol, který byl uveden v roce 2006. Protokol má v sobě zabudovány mechanismy TCP (využívá spojovaný přenos, ale nevyužívá spolehlivostní mechanismy TCP, u kterých dochází k velkým zpožděním). Hlavní vlastností protokolu je mechanismus, který brání zahlcení přenosových tras. DCCP je určen především pro aplikace, jako jsou streamované přenosy, kde hraje velkou roli zpoždění. Další vlastnosti je potvrzení o doručení odesílateli, multi-homing a multi-streaming. [18]

## 10 PŘENOS V REÁLNÉM ČASE

Systém pracující v reálném čase (Real-time systém). Základním požadavkem přenosu v reálném čase je nejen výsledek přenosu, ale především doba přenosu. Zpráva musí být přenesena v co nejkratším úseku. Mezní hranice této doby je nazývána deadline. Deadline reprezentuje akceptovatelný časový okamžik k dokončení. Dělíme jej do dvou skupin:

- **Hard deadline** – určitý časový interval nesmí být překročen, v opačném případě nastává závažná chyba, která už nemá pro uživatele žádnou hodnotu
- **Soft deadline** – určitý časový interval by neměl být překročen, pokud dojde k překročení, nenastává tak závažná chyba jako u hard deadline. [8]



Obr. 10.1: Rozdělení Deadline

### 10.1 Protokoly pro multimedia

#### 10.1.1 RSVP protokol

Protokol RSVP (Resource Reservation Setup Protocol), je signalizační protokol transportní vrstvy, který slouží k vyhrazení kapacit síťového přenosu. Komunikaci v protokolu RSVP iniciují příjemci, nikoliv odesílatelé. Z hlediska architektury sítě běží protokol RSVP nad protokolem IP.



Zprávu iniciuje hostitelský uzel jménem příslušné aplikace. Uzel provede 2 úkony. Zaprvé vyhodnotí zprávu RSVP, podle níž zjistí, zda může provést požadovanou rezervaci prostředků. Výsledek tohoto vyhodnocení závisí na dostupnosti prostředků. Poté aktualizuje informace a požadavek se předá od odesílatele k příjemci. Rezervační požadavky se musejí periodicky obnovovat. [16]

### **10.1.2 RTP protokol**

Protokol RTP (Real-time Transport Protocol) poskytuje mechanismy pro koncové multimediální přenosy v reálném čase, jako jsou například VoIP (Voice over Internet Protocol), VoD (Video on Demand), a jiné. [16]

Mechanismy pro podporu přenosu v reálném čase definujeme na aplikační vrstvě. RTP není závislý na protokolech nižších vrstev a podporuje jednosměrné i více-směrné vysílání.

### **10.1.3 RTCP protokol**

Tento protokol slouží ke kontrole a řízení celého přenosu a udává zpětnou odezvu na příchozí RTP pakety. Používá pro přenos protokol UDP a zajišťuje kvalitu služeb a odhad velikosti relace. Informace posílá na portu o jedna vyšší než protokol RTP. [16]

Zajišťuje statistické informace o protokolu RTP a o kvalitě jejich služeb. Šířka pásma RTCP nesmí přesáhnout 5 procent celkové šířky pásma pro spojení RTP.

### **10.1.4 RTSP protokol**

Protokol RTSP (Real Time Streaming Protocol) byl vyvinut pro řízení doručení dat v reálném čase audio a video obsahu. Je implementován prostřednictvím transportního protokolu s opravou chyb. RTSP je protokol řízení, společně s protokolem RTP (Real Time Protocol) umožňuje doručení dat klientům.

RTSP využívá transportní protokol TCP a port 554. Protokol také podporuje ovládací funkce přehrávače (např. metody, spuštění datového toku, pozastavení nebo ukončení vysílání dat. [16]

## 11 BEZDRÁTOVÝ PŘENOS S VYUŽITÍM TECHNOLOGIE WI-FI DIRECT

### 11.1 Wi-Fi Direct

Je to sada softwarových protokolů, která poskytuje přímou bezdrátovou komunikaci mezi dvěma zařízeními, bez nutnosti třetího propojovacího zařízení (například AP). Zařízení s touto certifikací mohou být připojena i ke skupině několika zařízení současně. Wi-Fi Direct připomíná režim Ad-hoc, je to ovšem technologie s vyšším výkonem a lepším zabezpečením (šifrování WPA2). [11]

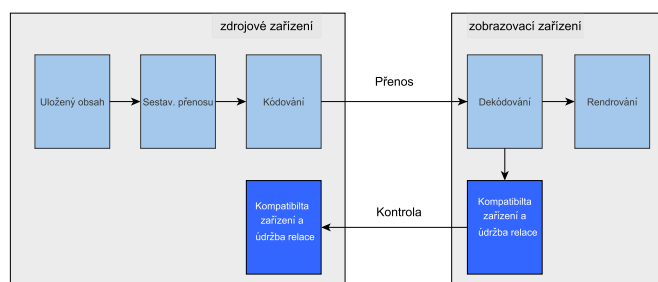
### 11.2 Miracast

Miracast je nový certifikovaný standard od organizace Wi-Fi Alliance. Miracast využívá bezdrátovou technologii Wi-Fi Direct pro přenos A/V streamu přímým spojením (peer-to-peer) dvou zařízení. Výhodou je, že data nemusí putovat přes přístupový bod. Zařízení na obou stranách musí obsahovat podporu této technologie. Podporuje rozlišení až 1080p. Je to náhrada kabelové varianty HDMI.

#### Sestavení relace

Miracast relace začíná žádostí uživatele. Datový obsah musí být přítomný na zdrojovém zařízení, aby mohl být prostřednictvím streamu přenesen na zobrazovací zařízení. Jakmile je obsah připraven k přenosu, zdrojové zařízení identifikuje dostupné zařízení a vyzve uživatele, aby zvolil zařízení, které bude působit jako display.

Dále zdrojové zařízení vytvoří spojení se zobrazovacím zařízením, v rámci přípravy na přenos. Jakmile je spojení navázáno, zdrojové zařízení kóduje posílaný obsah. Optimalizuje přenos podle aktuálního stavu kanálu na bezdrátovém médiu. Zobrazovací zařízení signál dekóduje a následně jej renderuje. [15]



Obr. 11.1: Sestavení relace standardu Miracast

## 11.3 WiDi – Wireless Display

Je to technologie pro bezdrátové připojení obrazovek. Jejím hlavním cílem je především snadné připojení televize a notebooků. Komunikace probíhá pomocí standardu Miracast. WiDi je technologie od společnosti Intel, která je podporována od verze čipu založené na architektuře Sandy Bridge a dále podporován vyššími modely.

Důležitou vlastností je podpora hardwarového enkodéru Quick Sync. Technologie WiDi je zaměřená především na streamovaný přenos videa, u kterého se klade důraz na zpoždění. To se pohybuje u technologie Sandy Bridge kolem 250 ms a u Ivy Bridge okolo 60 ms. Další vlastností Wireless Display je podpora USB zařízení (např. myš), které můžeme připojit k televizi a snadněji tak ovládat počítač na dálku. [9]



Obr. 11.2: Detekování dostupných zařízení s technologií WiDi

Na obrázku 11.2 je ukázán dostupný bezdrátový adaptér (televize LG), s implementovanou technologií WiDi. Po potvrzení žádosti je počítačem vygenerován a na televizi poté zobrazen čtyřmístný kód pro autentizaci.

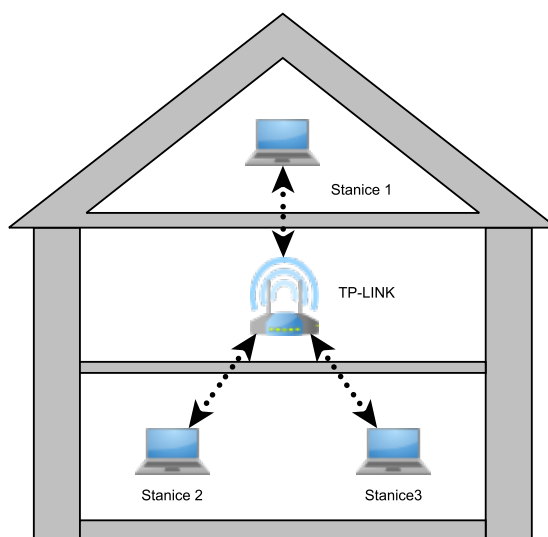
Relace byla vytvořena jen pro ilustraci WiDi a pro orientační zjištění dosahu této technologie. Vzdálenost, do které byl provoz konstantní se pohybovala kolem 4 metrů. Tato technologie byla zmíněna jen okrajově, bez podrobnějších měření.

## 12 PRAKTICKÁ ČÁST PRÁCE

### 12.1 Řešení problematiky skrytého uzlu

Wi-Fi bylo původně navrženo pro vnitřní prostory a předpokládala se viditelnost jednotlivých zařízení. V této praktické ukázce byla zapojena síť ve třípatrovém domě, kde byl router (TP-Link) umístěn v prostředním patře.

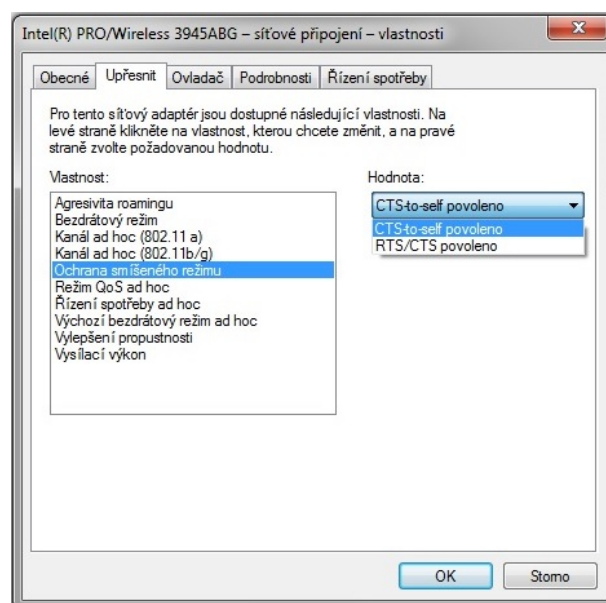
V prvním patře byly umístěny 2 stanice, které byly připojeny k síti TP-Link. Na těchto stanicích byl spuštěn test propustnosti reprezentovaný transportním nespolehlivým protokolem UDP pomocí programu iperf. Ve 3. patře byla do téže sítě napojena další stanice, která slouží k vytížení linky pomocí streamování videa z internetu. Stanice z 1. patra nevidí přes 2 podlaží na stanici do 3. patra. V těchto případech nastává situace, která se nazývá problém skrytého uzlu. Řešit jej můžeme buď softwarově nebo hardwarově. Obě tyto řešení mají své pro a proti.



Obr. 12.1: Schéma domu pro ilustraci skrytého uzlu

Router komunikuje se všemi zařízeními a může docházet ke vzájemnému rušení, pokud stanice komunikují ve stejnou dobu. V těchto případech může nastat značná ztrátovost.

Pro ověření těchto výpovědí byly nastaveny 3 režimy provozu. Režim CTS-to-self, režim RTS/CTS a smíšený režim (na stanicích 2 a 3 bylo nastaveno RTS/CTS a na stanici 1 režim CTS-to-self). Byly provedeny 4 měření na každé nastavení. Měřený úsek trval vždy 30 s. Komunikace probíhala přes router podporující standard 802.11g. V dnešní době již starší standard, ale v domácnostech stále ještě hojně využívaný.



Obr. 12.2: Nastavení režimů

### 12.1.1 Softwarové řešení

Je to jednodušší, méně nákladná varianta. Na routeru se nastavuje hodnota RTS Threshold, která nám udává minimální velikost přenášených paketů, pro které se začne využívat metoda RTS/CTS. RTS Threshold se nastavuje, aby se při přenosu malých paketů zbytečně nezatěžovala síť.

#### Režim CTS-to self

Tab. 12.1: Tabulka hodnot u režimu CTS-to-self

Číslo měření (30s)	1.	2.	3.	4.	Průměrná hodnota
Propustnost [kb/s]	883	934	1338	1090	1061
Ztrátovost [%]	43	42	39	40	41

#### Režim mix (na každém počítači rozdílné nastavení)

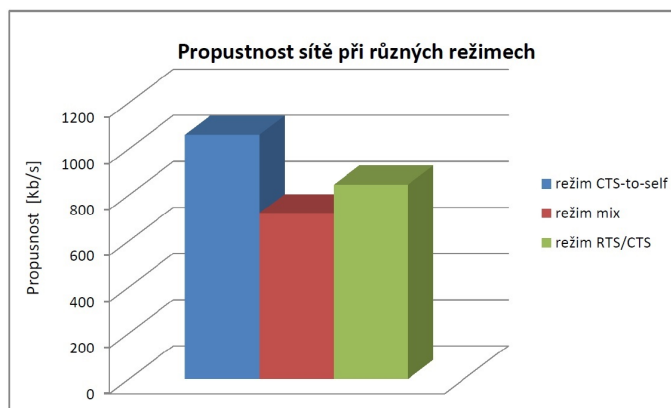
Tab. 12.2: Tabulka hodnot u smíšeného režimu

Číslo měření (30s)	1.	2.	3.	4.	Průměrná hodnota
Propustnost [kb/s]	557	759	795	754	721
Ztrátovost [%]	50	45	40	44	44,75

## Režim RTS/CTS

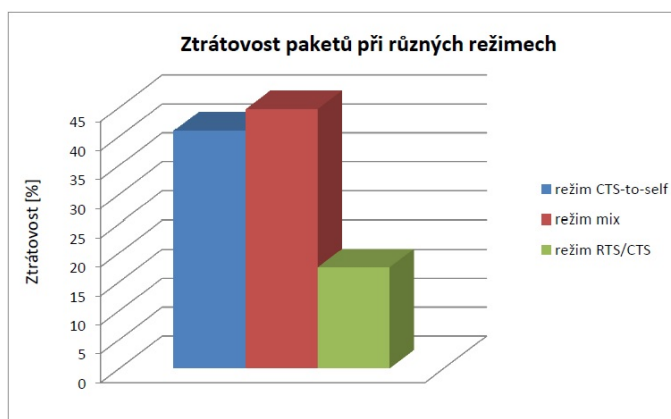
Tab. 12.3: Tabulka hodnot u režimu RTS/CTS

Číslo měření (30s)	1.	2.	3.	4.	Průměrná hodnota
Propustnost [kb/s]	934	831	775	843	845
Ztrátovost [%]	12	17	23	18	17,5



Obr. 12.3: Graf propustnosti

V grafu srovnání propustností při použití různých režimů, jde vidět, že největší propustnost měl režim CTS-to-self a to 1061 kb/s. Režim RTS/CTS měl reálnou propustnost o 21 % horší, z důvodu posílání služebních paketů. Nejhuře dopadl smíšený režim, kde propustnost poklesla o 32 %.



Obr. 12.4: Graf ztrátovosti

V grafu srovnání ztrátovosti při různých režimech dopadl nejlépe režim RTS/CTS s průměrnou ztrátovostí paketu 17,5 %. Režim CTS-to-self dosáhl ztrátovosti až 41 % a smíšený režim dokonce 44,75 % ztracených paketů.

## Nastavení hodnoty RTS Threshold

Tovární nastavení této hodnoty je 2347 bytů. To znamená, že by metoda RTS/CTS neměla žádný smysl, protože by byla umožněna pouze u paketů větších než tato hodnota. Opačná varianta nastavení RTS Threshold na nulovou hodnotu by znamenala, že se bude metoda RTS/CTS používat vždy. V tomto nastavení však není možná, minimální hodnota je 256. Důležité je ovšem nastavit hodnotu Threshold na všech síťových zařízeních.

The image shows a screenshot of a router's web interface, specifically the 'Wireless Advanced' settings page. On the left is a sidebar menu with options like Status, Quick Setup, WPS, Network, Wireless (selected), and others. The main area is titled 'Wireless Advanced' and contains several configuration fields. The 'RTS Threshold' field is highlighted with a red rectangular box and shows the value '512' with a range '(256-2346)' next to it. Other visible settings include 'Transmit Power' set to 'High', 'Beacon Interval' at '100', 'Fragmentation Threshold' at '2346', and 'DTIM Interval' at '1'. There are also three checkboxes: 'Enable WMM' (checked), 'Enable Short GI' (unchecked), and 'Enable AP Isolation' (unchecked). A 'Save' button is located at the bottom right of the settings area.

Obr. 12.5: Nastavení hodnoty RTS Threshold

U předešlých měření byla na routeru TP-Link nastavena hodnota RTS Threshold na velikost 512 bytů. Pomocí programu Wireshark byl zachycen probíhající provoz a byly procentuálně analyzovány délky paketů. Tato varianta byla zvolena, aby režie u malých paketů nebyla příliš vysoká a nezatěžovala tak provoz. Pakety menší než hodnota 512 bytů využívaly pouze CSMA/CA a nezasílaly tak komunikační požadavky RTS/CTS.

### 12.1.2 Hardwarové řešení

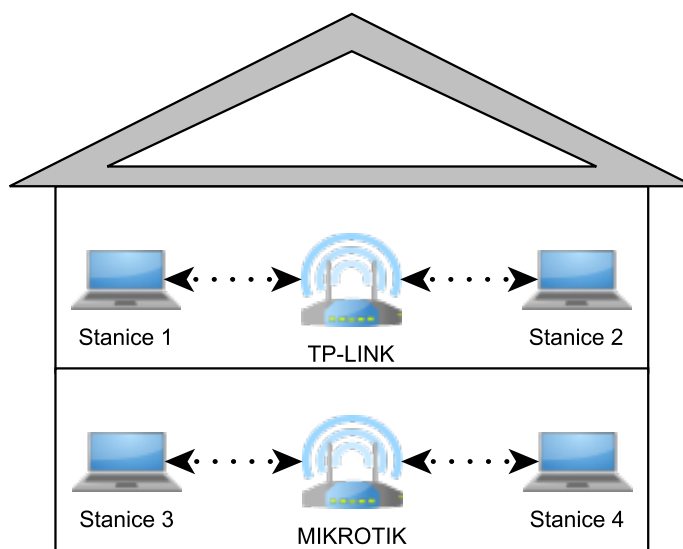
Spočívá v nahrazení spojů point-to-multipoint spojením point-to-point a tedy přímé propojení dvou spojů. To znamená, že vyhradíme dvojici Wi-Fi adaptérů a dvojici směrových antén pro každou spojovou cestu.

Výhodou řešení je vyšší přenosová rychlost. Je to účinné řešení, ale je cenově nákladné a nelze použít při větším počtu klientů. [19]

## 12.2 Výběr a optimalizace vhodného kanálu

Jeden z nejčastějších důvodů rušení a dokonce i výpadků bezdrátové sítě je rušení od okolních Wi-Fi sítí. Pokud komunikuje více sítí na stejném nebo sousedním kanále, mohou vznikat přeslechy, ztráty či výpadky spojení. V této kapitole je provedeno názorné měření a pozorování vzájemného rušení okolních sítí a vlivů na rychlost a kvalitu přenosu.

Tyto případy mohou nastat například v bytových domech, kde je více účastníků bezdrátového provozu. V kapitole 4.0.1 bylo uvedeno, že v České Republice máme pouze 3 samostatné kanály, které se nepřekrývají a minimální odstup mezi jejich centrálními frekvencemi je 25 MHz. Této podmínky lze ovšem stěží dosáhnout v praxi. Nemluvě o routerech využívající šířky pásma 40 MHz.



Obr. 12.6: Schéma domu pro ilustraci překrývání kanálů

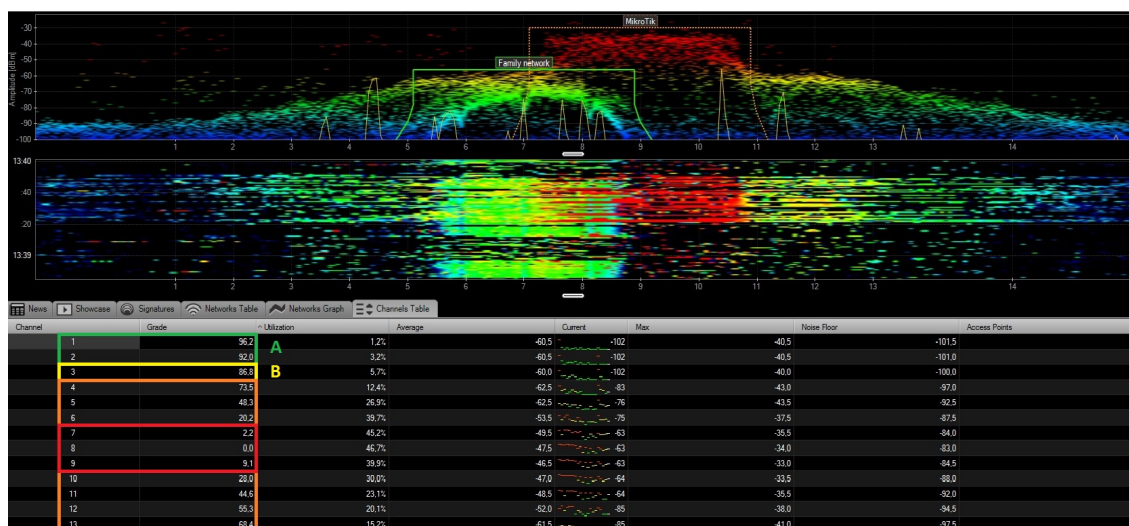
### 12.2.1 Měření vzájemného rušení jednotlivých kanálů

V tomto praktickém příkladě bylo zapojení provedeno ve dvoupodlažním bytovém domě, kde v prvním patře byla vytvořena síť Family network a v přízemí síť Mikrotik. Vzájemné umístění routerů bylo pod sebou.

Síť Family network (použitý router TP-Link), byla po celou dobu měření umístěna na 7. kanále a bylo zde simulováno vytížení sítě provozem mezi stanicemi 1 a 2. Tento provoz byl reprezentován nespolehlivým protokolem UDP s konstantní přenosovou rychlostí 2 Mbit/s. Tyto parametry se neměnily po celou dobu měření.



Síť Mikrotik byla nastavena na kanále 8 a postupně se posouvala až na kanál 12. K síti byly připojeny stanice 3 a 4, mezi nimiž probíhal test propustnosti pomocí programu iperf s použitým protokolem UDP. Byly provedeny celkem 4 měření na všech definovaných kombinacích překrývajících se kanálů, tj. 7. a 8. až 7. a 12. kanál, kde byla splněna podmínka rozestupu 25 MHz a tedy by zde nemělo docházet k vzájemnému rušení. Doba každého dílčího měření byla 30 s.



Obr. 12.7: Schéma překrývání wi-fi sítí se středovým kanálem 7 a 9

Na obrázku 11.7 jsou znázorněny úrovně signálu (Grade), kde hodnoty 90 a vyšší patří do kategorie A, hodnoty 80 – 90 patří do kategorie B. Pokud úroveň klesne pod hodnotu 70, nedoporučuje se umísťovat bezdrátovou síť. V našem případě se tedy další síť doporučuje umístit pouze na kanál 1, 2 nebo 3. Z těchto důvodů máme tedy jen omezené možnosti. Chanalyzer byl umístěn v přízemí.

Tab. 12.4: Porovnání propustnosti u překrývajících se kanálů

Měřené kanály	Dílčí měření propustnosti [kb/s]				
	1.	2.	3.	4.	Průměrná hodnota
<b>7 a 8</b>	1005	1226	1433	1210	1218
<b>7 a 9</b>	3923	4007	4018	4101	4012
<b>7 a 10</b>	7156	6059	5074	6163	6113
<b>7 a 11</b>	6927	6334	6542	6717	6630
<b>7 a 12</b>	7320	7273	6985	7606	7296

V tabulce jsou zaznamenány hodnoty testu propustnosti na síti Mikrotik mezi dvěma počítači. Z naměřených hodnot vyplývá, že nejmenší propustnost nastala

mezi kanály 7 a 8, kde byla mezera pouze jeden kanál (5 MHz).

U tohoto nastavení nastávaly výpadky a jejich možné vzájemné fungování bylo prakticky nemožné. Ve srovnání s ideálním nastavením, tedy s kanály 7 a 12, se propustnost sítě pohybovala pouze kolem 16 %.

U kanálů 7 a 9 se situace rapidně zlepšila. Propustnost stoupla na 54 % ideálních hodnot. Toto nastavení je reálně použitelné, výhodou je možnost vzájemné funkce 5 bezdrátových sítí. Další dvě nastavení měly už podobné výsledky, tedy 83 %, respektive 89 % a blížily se k ideálním hodnotám.

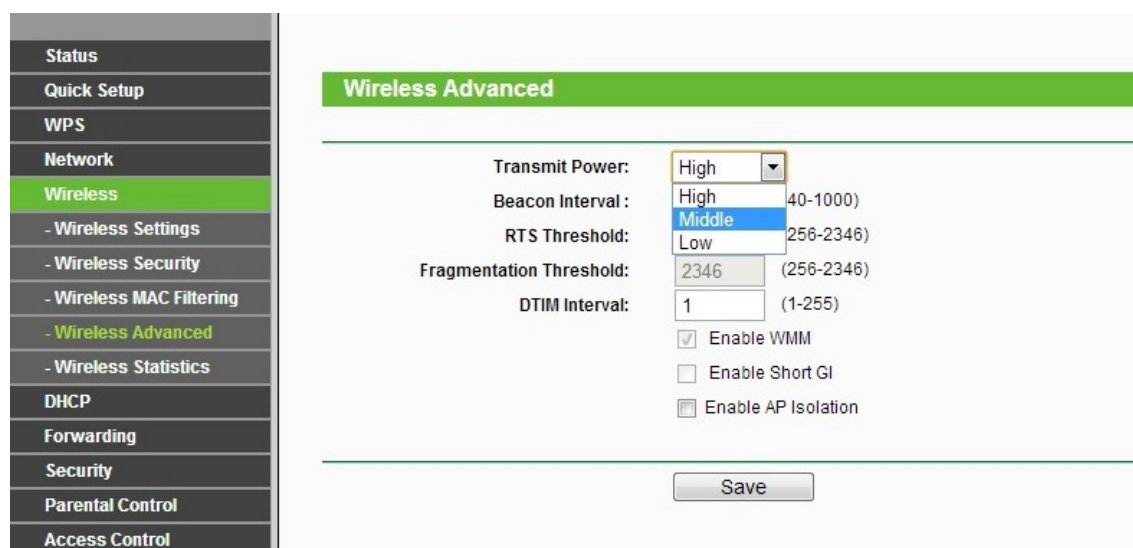
### **Možnosti řešení:**

- **Nastavení vysílacího výkonu**

Jedna z možností je upravení vysílacího výkonu jednotlivých směrovačů. Často se stává, že velký vysílací výkon zaruší okolní prostředí v desítkách metrů. Dokonce i když jsou sítě vzdáleny dostatečně daleko od sebe, mohou být takto zarušeny. Při nastavení nižšího vysílacího výkonu routeru sice snížíme dosah, ale zlepšíme kvalitu díky menšímu vzájemnému rušení. Nastavení se provádí na routeru.

Použité zařízení (TP-Link) nemělo přesně kvantifikované nastavení vysílacího výkonu, tudíž bylo pouze přepnuto do stavu Middle (výběr ze stavů Low, Middle a High). U routeru Mikrotik bylo nastavení celkového vysílacího výkonu sníženo ze 100 mW na 70 mW.

V tomto praktické příkladě nemělo snížení výkonu vliv na dostupnost signálu v bytě (byt 3+1). Mohou ovšem nastat případy, kdy snížení výkonu není možné (např. příliš tlusté zdi, velká plocha bytu atd.).

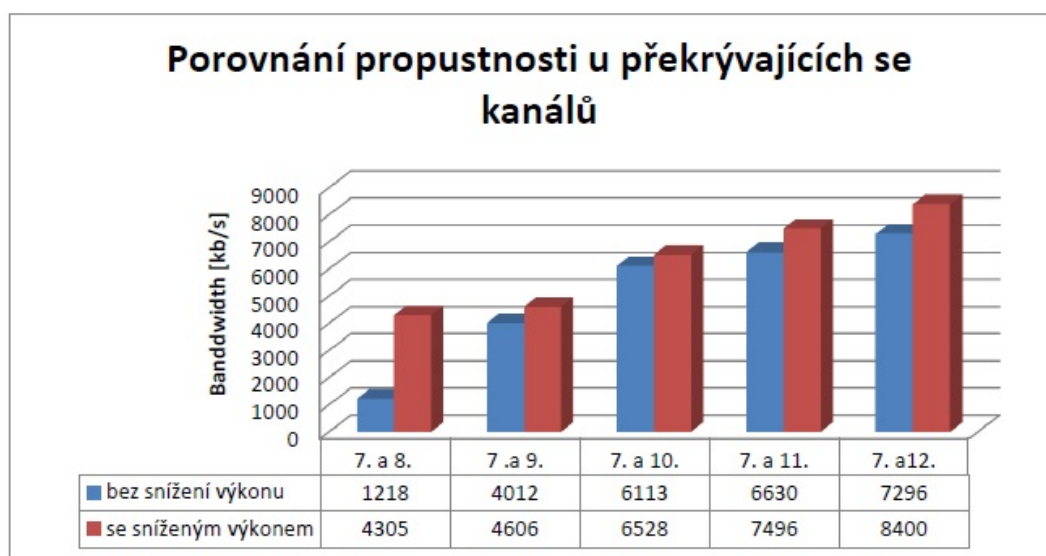


Obr. 12.8: Nastavení vysílacího výkonu routeru

Tab. 12.5: Porovnání propustnosti u překrývajících se kanálů (snížení vys. výkonu)

Měřené kanály	Dílčí měření propustnosti [kb/s]				
	1.	2.	3.	4.	Průměrná hodnota
<b>7 a 8</b>	3662	4590	5136	1210	3833
<b>7 a 9</b>	4352	4791	4833	4448	4606
<b>7 a 10</b>	6339	6296	6950	6527	6528
<b>7 a 11</b>	7359	7634	7409	7582	7496
<b>7 a 12</b>	8235	8656	8482	8227	8400

V tabulce 11.5 jsou zaznamenány hodnoty propustnosti při snížení vysílacího výkonu obou routerů. Výrazné zlepšení nastalo už u prvního nastavení, tedy u 7. a 8. kanálu. Propustnost se pohybovala kolem 45 % ideálního stavu. U dalších variant bylo zlepšení v porovnání s předchozím nastavením také viditelné.



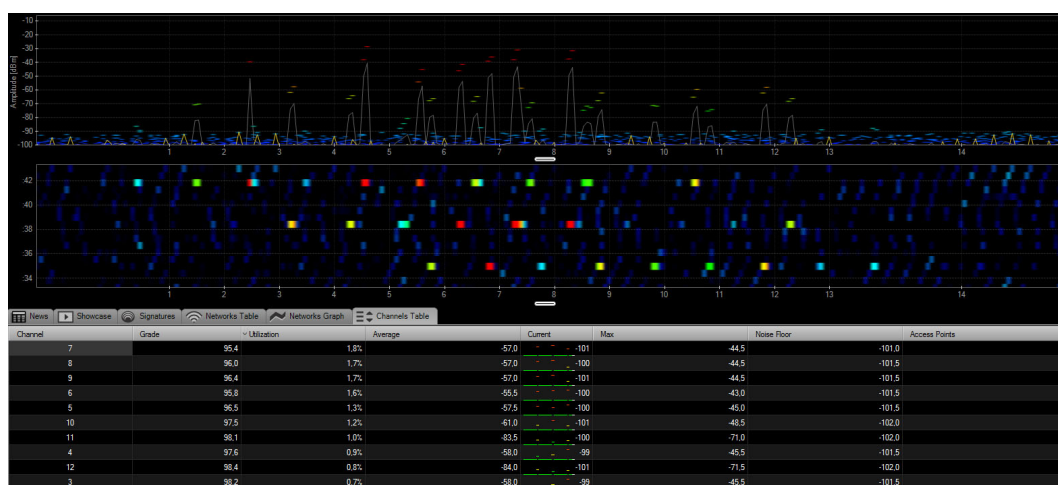
Obr. 12.9: Porovnání propustnosti při změně podmínek

Z grafu lze porovnat jednotlivé režimy zapojení (se sníženým výkonem routerů a bez něj). Ve všech variantách byla propustnost lepší u sníženého výkonu. Dokonce i překrývání kanálů 7 a 8 se sníženým výkonem bylo v praxi použitelné.

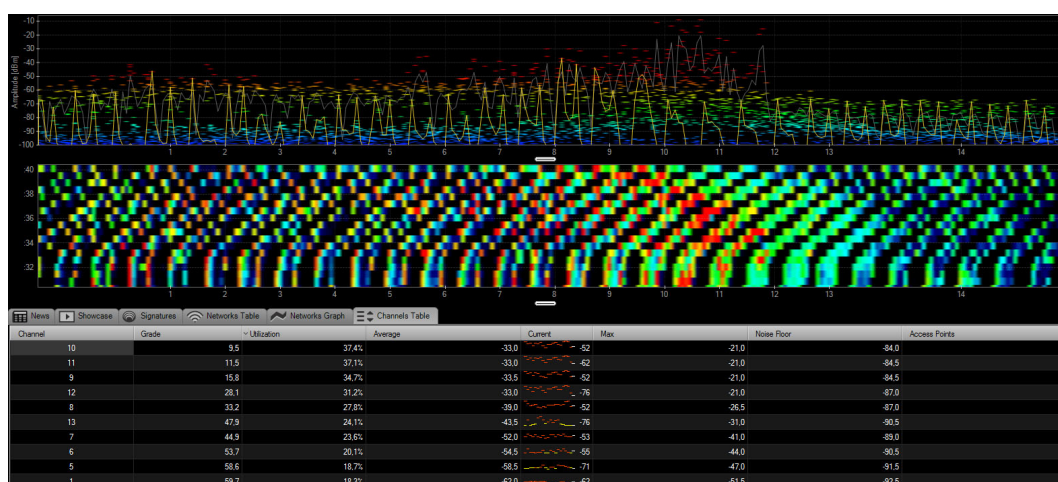
## 12.3 Další druhy rušení

### 12.3.1 Rušení mikrovlnnou troubou

Mikrovlnné trouby pracují v rozsahu pásma 2,4 GHz, kde také funguje standard 802.11 a tudíž může snadno nastat interference při vysílání různých zařízení na stejných frekvencích. Pomocí Chanalyzeru Wi-spy zjišťujeme stav na bezdrátovém mediu za klidných podmínek bez spuštění mikrovlnné trouby a také bez jakéhokoliv provozu bezdrátových sítí v okolí Chanalyzeru. Využití (Utilization) sítě v čase se pohybovalo okolo 2 %, obrázek 11.10.



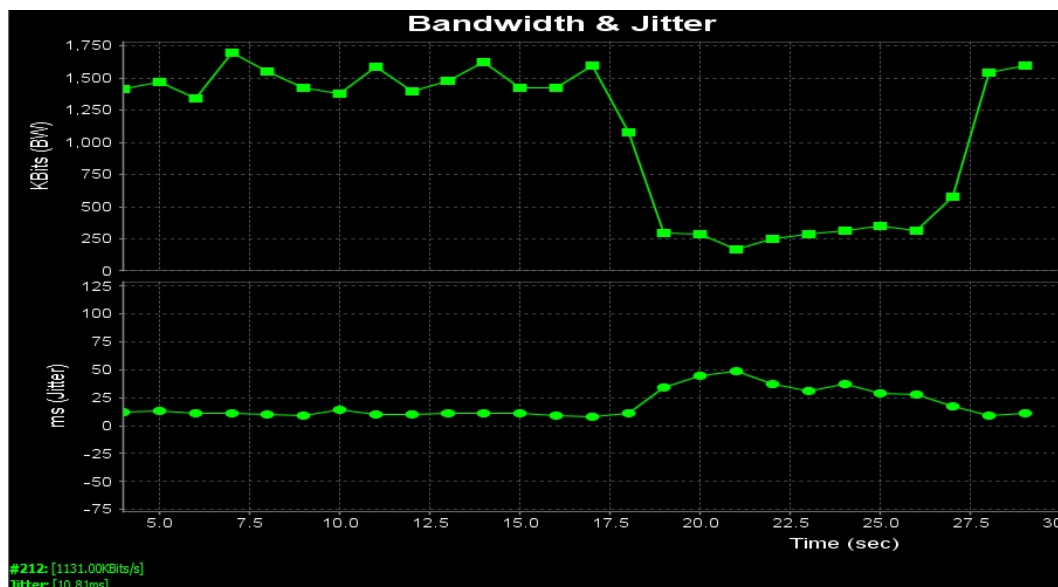
Obr. 12.10: Bezdrátové médium v klidovém stavu



Obr. 12.11: Bezdrátové médium při spuštění mikrovlnné trouby

Na obrázku 11.11 je rušení znatelné téměř v celé šířce pásma od zaznamenaných frekvencí, tedy v rozmezí 2400 MHz – 2470 MHz. Nejintenzivnější pak tedy na

kanálech 9, 10 a 11, kde dosahuje využití kanálu v čase okolo 37 %. Mikrovlnné amplitudové úrovně se liší v závislosti na jejich vzdálenosti od spektrálního analyzátoru. Vytvářejí obvykle tvar tzv. horského svahu. [17]



Obr. 12.12: Propustnost sítě při spuštění mikrovlnné trouby v programu jperf

Na obrázku 11.12 je zobrazena šířka pásma (bandwidth) a kolísání zpoždění (jitter) při testu propustnosti sítě mezi dvěma stanicemi pomocí programu jperf. V čase do 15 s byl na bezdrátovém médiu klid a provoz byl konstantní. Od 15 s byla spuštěna mikrovlnná trouba. Za tohoto stavu propustnost poklesla z 1500 kb/s na 250 kb/s.

Pro toto měření byl použit starší typ mikrovlnné trouby. V dnešní době jsou již mikrovlnné trouby velice dobře odstiňovány a nehrozí tedy problém s rušením bezdrátového provozu. Problémy ovšem vznikají u starších zařízení a musíme s nimi počítat.

### 12.3.2 Rušení Wi-Fi technologií Bluetooth

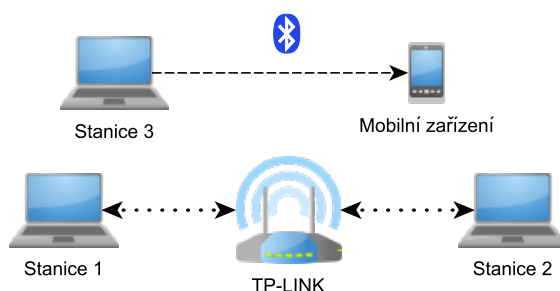
Obě tyto technologie pracují v pásmu 2,4 GHz a využívají rozprostřené spektrum signálu. Vysílač využívající technologii FHSS (Bluetooth) není pro přijímač využívající DSSS (Wi-Fi) nic jiného, než zdroj šumu nebo rušení. Silná interference může znamenat pokles signálu nebo může dokonce dojít až ke ztrátě spojení. Proto jsou zavedeny jisté metody, které dokáží tyto vlivy omezit. [21]

- **Frekvenční izolace:** funkce AFH (Adaptive Frequency Hopping) implementována v Bluetooth zařízení automaticky vyhledá pásmo, které je momentálně využíváno a přizpůsobí tomu svůj provoz.

- **Použití TDM(Time Division Multiplexing):** je to metoda soužití, která využívá princip střídavého vysílání u těchto dvou technologií.

### Praktické zjišťování vlivu vzájemného rušení Wi-Fi a Bluetooth

V tomto praktickém příkladě byla vytvořena síť PAN (Personal Area Network), mezi stanicí 3 a mobilním zařízením. Pomocí technologie Bluetooth 4.0 byl poslán soubor ze stanice 3 do mobilního zařízení. Souběžně byla ve stejné místnosti vytvořena Wi-Fi síť, ke které byly připojeny stanice 1 a 2, mezi kterými byl spuštěn test propustnosti.



Obr. 12.13: Schéma zapojení – rušení pomocí technologie Bluetooth

```
[212] local 192.168.0.113 port 5001 connected with 192.168.0.111 port 64393
[ ID] Interval      Transfer      Bandwidth      Jitter      Lost/Total Datagrams
[212] 0.0-10 sec    2.28 MBytes  1.94 Mbits/sec  13.176 ms   41/ 1666 (2.5%)
[212] local 192.168.0.113 port 5001 connected with 192.168.0.111 port 63856
[ ID] Interval      Transfer      Bandwidth      Jitter      Lost/Total Datagrams
[212] 0.0-10 sec    1.99 MBytes  1.65 Mbits/sec  10.158 ms   17/ 1435 (1.2%)
```

Obr. 12.14: Propustnost linky bez vnějšího rušení

```
[212] local 192.168.0.113 port 5001 connected with 192.168.0.111 port 58819
[ ID] Interval      Transfer      Bandwidth      Jitter      Lost/Total Datagrams
[212] 0.0-10 sec    119 KBytes   121 Kbits/sec  76.255 ms   21/ 104 (20%)
[212] local 192.168.0.113 port 5001 connected with 192.168.0.111 port 60321
[ ID] Interval      Transfer      Bandwidth      Jitter      Lost/Total Datagrams
[212] 0.0-10 sec    187 KBytes   146 Kbits/sec  86.984 ms   33/ 163 (20%)
```

Obr. 12.15: Propustnost rušené linky technologií Bluetooth

Byla provedena celkem 4 měření, 2 bez okolního rušení a 2 měření s rušením technologií Bluetooth. které jsou zaznamenány na obrázcích. Maximální ztrátovost u nerušené linky dosahovala 2,5 % ve srovnání s rušeným přenosem, kde ztrátovost dosáhla až 20 %. Propustnost linky bez zatížení dosáhla hodnoty 1,94 Mb/s, ovšem při Bluetooth provozu pouze hodnot 146 kb/s. Propustnost sítě se tedy snížila více než 10 krát.



## 13 VÝSLEDKY A ZHODNOCENÍ PRÁCE

### 13.1 Problematika skrytého uzlu

Z naměřených hodnot vyplývá, že při nastavení režimu CTS-to-self bylo sice dosaženo nejvyšší měřené propustnosti sítě (průměrná hodnota ze 4 měření byla 1061 kb/s). Vznikala zde ovšem obrovská ztrátovost při paketovém přenosu (v průměru až 41 %). Tato vysoká ztrátovost byla způsobena z důvodu, že se klienti vzájemně neviděli a nemohli tak časově synchronizovat své přenosy. Stanice vysílaly bez ohledu na další souběžně probíhající přenos.

Nastavení režimu mix dopadlo při srovnání s ostatními výsledky nejhůře. Průměrná propustnost dosáhla hodnoty 721 kb/s a ztrátovost paketů byla 44,75 %. Proto je velmi důležité nastavit jen jeden typ režimu na všechny připojené klienty v síti.

Režim RTS/CTS měl sice průměrnou propustnost 845 kb/s, tedy menší než režim CTS-to-self, z důvodu zasílání komunikačních požadavků RTS/CTS. Ovšem ztrátovost zde razantně poklesla na hodnotu 17,5 % ztracených paketů. Těmito zjištěními byly potvrzeny teoretické poznatky o problémech skrytého uzlu.

#### **Doporučení pro nastavení:**

Režim CTS-to-self je tedy vhodný nastavit pro menší sítě, kde je zaručena viditelnost mezi jednotlivými zařízeními. Hodnotu Threshold ponechat na největší možné hodnotě. Pokud se jedná o venkovní síť nebo síť o velké rozloze, je vhodné nastavit všechna připojená zařízení do režimu RTS/CTS a hodnotu Threshold nastavit v rozmezí (512 – 1024) bytů. Dále pak zkontrolovat, aby měla všechna zařízení nastaven stejný režim.

### 13.2 Výběr a optimalizace vhodného kanálu

V dnešní době je stále více účastníků bezdrátového provozu v sítích 2,4 GHz, toto pásmo má ovšem pouze omezené možnosti. Toto praktické měření demonstrovalo problematiku rušení od okolních bezdrátových sítí v bytových domech a možné varianty řešení tohoto problému. Jsou situace, kdy je pásmo tak silně zarušeno, že je provoz téměř nemožný a spousta uživatelů musí sáhnout po metalické variantě. Jsou však možnosti, které mohou přispět k optimalizaci těchto bezdrátových sítí a jejich funkčnost může být zachována.

Z měření vyplynulo, že nastavení nižších vysílacích výkonů routerů má velký vliv na vzájemné rušení. Toto nastavení by ovšem nemělo žádný smysl, kdyby se

nastavovalo pouze na jednom směrovači, z těchto důvodů hraje také velkou roli i například domluva se sousedy na snížení vysílacího výkonu routerů.

Pro správný výběr optimálního kanálu, je potřeba zvážit další faktory. Jeden z nich je zjištění volného kanálu například dostupným programem inSSIDer. Pro ještě důkladnější poznatky o stavu bezdrátového média je vhodné použít například Wi-Fi Spy Chanalyzer, který je schopen zjistit, jaké je aktuální vytížení kanálu. Toto zjištění je velmi důležité, neboť jenom překrývání různých Wi-Fi sítí ještě není zárukou vzniku rušení. Je možné zjistit, jak jsou kanály vytěžovány účastníky bezdrátového provozu například v průběhu dne. Díky těmto poznatkům lze nastavení vlastní sítě lépe optimalizovat.

### 13.3 Další druhy rušení

Byly také porovnány další možnosti rušení v pásmu 2,4 GHz. První z nich byla simulace provozu při spuštění mikrovlnné trouby. Byl opět proveden test propustnosti mezi dvěma stanicemi. Z grafu na obrázku 11.12 je vidět, že propustnost poklesla na pětinou hodnotu ve srovnání s klidovým stavem. Tyhle problémy nastávají u vlastníku starších mikrovlnných trub. Nové zařízení jsou velice dobře odstiňovány.

Za zmínku stojí také test rušení dětskými chůvičkami. Wi-Fi síť však nebyla prakticky vůbec ovlivněna. Díky nízkým vysílacím výkonům byl rozdíl propustností při rušení a bez něj téměř zanedbatelný.



## 14 ZÁVĚR

Bakalářská práce byla zaměřena na technologie podporující přenosy v bezdrátových sítích 802.11 a na druhy rušení které tyto přenosy ovlivňují. Práce byla rozdělena na dvě hlavní části. První část se věnovala teoretickému rozboru a porovnání jednotlivých standardů 802.11, jeho rozšíření a popis přístupových metod.

Dále byly porovnány mechanismy QoS a qWave, které slouží ke zkvalitnění provozu v bezdrátových sítích. Velký rozdíl mezi těmito technologiemi je ve využití, jelikož sada qWave je určena výhradně pro použití v domácích bezdrátových sítích a není zaměřena na podnikové sítě.

Pro přenosy multimediálních dat byly porovnány protokoly TCP a UDP a uvedeny jejich výhody, nevýhody a vlivy na přenos. Dále je podrobně popsán protokol SCTP a jsou zde uvedeny jeho vlastnosti. Jen okrajově byly zmíněny technologie podporující bezdrátový přenos Peer-to-Peer, Wi-Fi Direct.

V praktické části této práce byl simulován bezdrátový provoz ve tří patrovém domě, kde nastával problém skrytého uzlu. Byl ověřen mechanismus bránící těmto komplikacím. Z měření vyplynulo, že ztrátovost přenosu při použití mechanismu RTS/CTS byla téměř o 26% menší než u režimu CTS-to-self, ovšem propustnost byla díky větším požadavkům na provoz nižší. Dále bylo z měřených hodnot zjištěno, že je důležité tyto režimy nekombinovat a zvolit jen jeden z nich. Pro geograficky malé sítě nemá režim RTS/CTS smysl, jen zvyšuje její zatížení. U velkých sítí, kde je riziko, že by se stanice nemuseli vidět, vhodné režim RTS/CTS nastavit. Uvedena byla i hardwarová varianta řešení, která je ovšem drahá a omezená počtem účastníků.

Dále pak byly zkoumány vlivy vzájemného rušení dvou bezdrátových sítí v pásmu 2,4 GHz, které mohou zapříčinit snížení propustnosti nebo dokonce výpadky připojení. Tento problém může nastat například v bytových domech, kde je více účastníků provozu. V této práci bylo toto prostředí simulováno a byly provedeny testy propustnosti na výše uvedené varianty nastavení. Z naměřených hodnot bylo zjištěno, že propustnost sítě byla dostatečná již při rozestupu 2 kanálů od jejich centrálních frekvencí. Toto zjištění nám umožňuje funkci 5 bezdrátových sítí, které mohou fungovat současně.

Při variantě snížení vysílacích výkonů routerů bylo dosaženo mnohem lepších hodnot propustnosti sítě a dokonce bylo možné provozovat síť bez velkého vlivu rušení i při rozestupu pouze jednoho kanálu (5 MHz). Tím vzrostl možný počet vzájemně fungujících sítí. Snížení vysílacího výkonu routerů nijak neovlivnilo dosah sítí v uvedeném případě (byty 3+1). Z naměřených hodnot plyne závěr, že maximální vysílací výkon ještě není zárukou kvalitního signálu. Proto je v případě problémů důležitá i dohoda se sousedy o nastavení těchto vysílacích výkonů. Na závěr byly porovnány další možnosti externího rušení (mikrovlnná trouba, technologie Bluetooth

4.0), kde bylo měřením zjištěno snížení propustnosti sítě 2,4 GHz a tudíž musíme s těmito problémy při bezdrátovém provozu také počítat.

Tato práce měla ukázat, že rušení bezdrátových sítí může být dosti závažnou věcí. Mnoho uživatelů, kteří síť používají jen jako přístup k internetu sice tyto problémy často ani neřeší a spokojí se s provozem, jaký je. Pro ty, co síť využívají multimediálně je optimalizace nezbytná.

# LITERATURA

- [1] KALLAY, Fedor. *Počítačové sítě a jejich aplikace*. Praha: Grada Publishing, 2003. ISBN 80-247-0545-1.
- [2] Quality Windows Audio-Video Experience. *WinHEC 2004 Version* [online]. april 13, 2004, s. 12 [cit. 2012-11-21]. Dostupné z: <http://www.mojotoys.com/docs/qWave.doc>
- [3] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 2. aktualiz. vyd. Brno: Computer Press, 2006, 430 s. ISBN 80-251-1278-0.
- [4] TULLOCH, Mitch. *Microsoft Windows Vista Resource Kit*. Vyd. 1. Brno: Computer Press, 2008, 2 sv. (782, 648 s.). ISBN 978-80-251-1990-712.
- [5] Wi-Fi Alliance. Wi-Fi CERTIFIED™ for WMM™ - *Support for Multimedia Applications*. [Online] 1. září 2004. [Citace: 19. listopadu 2012.], dostupné z: <http://www.wi-fi.org>
- [6] WALKE, Bernhard H, Stefan MANGOLD a Lars BERLEMANN. *IEEE 802.11 wireless systems: protocols, multi-hop mesh/relaying, performance and spectrum coexistence*. Chichester: John Wiley, 2006, xix , 382 s. ISBN 04-700-1439-3.
- [7] CARROLL, Brandon. *Bezdrátové sítě Cisco: autorizovaný výukový průvoce*. 1. vyd. Brno: Computer Press, 2011, 478 s. Samostud. ISBN 978-80-251-2884-8.
- [8] ČÍKA, Petr. *Multimediální služby* [online]. 1. vyd. 2012 [cit. 2012-12-11]. 129 s. ISBN 978-80-214-4443-0.
- [9] OLŠAN, Jan. *WiDi 3.5*. [online]. [cit. 2013-05-14]. Dostupné z: <http://extrahardware.cnews.cz/widi-35-intel-vylepsil-bezdratovy-prenos-obrazu-nove-podporuje-miracast>
- [10] RÄISÄNEN, Vilho. *Implementing service quality in IP networks*. Chichester: John Wiley, 2003, xxvii, 325 s. ISBN 04-708-4793-X.
- [11] DOUPAL, František. *Wi-Fi Direct*. [online]. [cit. 2013-05-04]. Dostupné z: <http://notebook.cz/clanky/technologie/2010/wi-fi-direct>
- [12] STEWART, R. *SCTP Authentication Chunk. Authenticated Chunks for the Stream Control Transmission Protocol* [online]. září 2007, s. 19 [cit. 2013-04-09]. Dostupné z: <http://www.ietf.org/rfc/rfc4895.txt>

- [13] MORROW, Robert. *Wireless network coexistence*. New York: McGraw-Hill, 2004, xvii, 444 s. ISBN 00-713-9915-1.
- [14] LÁTAL a VANDERKA. *Simulace a plánování vnitřního pokrytí budov dle standardu IEEE 802.11 v prostředí softwarové aplikace I-Prop-1 část*. [online]. 2011, č. 44, s. 13 [cit. 2013-05-20]. Dostupné z: <http://www.elektrorevue.cz/>
- [15] WI-FI CERTIFIED MIRACAST™. Extending the Wi-Fi experience to seamless video display. [online]. [cit. 2013-05-20]. Dostupné z: [www.wi-fi.org](http://www.wi-fi.org)
- [16] NAIK, D. *Internet standardy a protokoly*. Vyd. 1. Brno: Microsoft Press, 1999, 302 s. ISBN 80-722-6146-0
- [17] *Interference Identification Guide*. [online]. [cit. 2013-05-02]. Dostupné z: <http://files.metageek.net/support/Interference>
- [18] CHOWDHURY. *Performance Analysis of Datagram Congestion Control Protocol (DCCP)*. [online]. 2011, roč. 3, č. 5 [cit. 2013-05-31]. Dostupné z: <http://dc492.4shared.com/doc/r-hNmE1k/preview.html>
- [19] TANGERO. *Problém skrytého uzlu*. [online]. 2012 [cit. 2013-04-23]. Dostupné z: [http://www.marigold.cz/wifi/doku.php/problem\\_skryteho\\_uzlu](http://www.marigold.cz/wifi/doku.php/problem_skryteho_uzlu)
- [20] XIAO, Yang. *Performance Analysis of the IEEE 802.11e Block ACK Scheme in a Noisy Channel* [online]. [cit. 2013-05-26]. Dostupné z: <ftp://ftp-sop.inria.fr/rodeo/turletti/broadnets05.pdf>
- [21] *20 Myths of Wi-Fi Interference*. [online]. [cit. 2013-05-22]. Dostupné z: <http://www.cisco.com/en/US/prod/collateral/wireless>
- [22] MOLNÁR, Karol. *Hardware počítačových sítí*. Vyd. 1. Brno: Vysoké učení technické v Brně Fakulta elektrotechniky a komunikačních technologií Ústav telekomunikací, 2012. 157 s. ISBN 978-80-214-4449-2.
- [23] CHOI, Sunghyun. *IEEE 802.11e Contention-Based Access Channel (EDCF) Performance Evaluation*. [Online]. 2007, s. 6. [cit. 2013-04-16]. Dostupné z: <http://www.cs.jhu.edu>

# SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ACK Acknowledge

AFH Adaptive Frequency Hopping

AIFS Arbitration Interframe Space

AP Access Point

API Application programming interface

BSS Basic Service Set

CFP Contention-Free Period

CP Contention Period

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

CTS Clear To Send

DCCP Datagram Congestion Control Protocol

DCF Distributed Coordination Function

DIFS Distributed Interframe Space

DS Distribution System

DSSS Direct Sequence Spread Spectrum

EDCF Enhanced Distribution Coordination Function

ESS Extended Service Set

ETSI European telecommunication standards institute

FHSS Frekvence-hopping spread spectrum

GQoS Generic Quality of Service

HC Hybrid Coordinator

HCF Hybrid Coordination Function

HD High Definition

HDRV High Definition Television

IBSS Independent Basic Service Set

IEEE Institute of Electrical and Electronics Engineers

IP Internet Protocol

LAN Local Area Network

LLTD Link -Layer Topology Discovery

MAC Media Access Control

MIMO Multiple-Input Multiple-Output

NAV Network Allocation Vector

OFDM Orthogonal Frequency Division Multiplex

PAN Personal Area Network

PCF Point Coordination Function

qWave Quality of Service

QoS Quality of Windows Audio/Video Experience

RF Radio Frequency

RPC Remote Procedure Call

RSVP Resource Reservation Setup Protocol

RTS Request To Send

RTCP Real-time Transport Control Protocol

RTP Real-time Transport Protocol

RTSP Real-time Transport Streaming Protocol

SBM Subnet Bandwidth Manager

SCTP Stream Control Transmission Protocol

SDTV Standard Definition Television

TC Traffic Control

TCP Transmission Control Protocol

TDM Time Division Multiplexing

UDP User Datagram Protocol

UNII Unlicensed National Information Infrastructure

VoD Video on Demand

VoIP Voice over Internet Protocol

WiDi Wireless Display

Wi-Fi Wireless Fidelity

WDS Wireless Distribution System

WLAN Wireless Local Area Network

WMM Wi-Fi Multimedia

# SEZNAM PŘÍLOH

A Obsah elektronické přílohy

65



## **A OBSAH ELEKTRONICKÉ PŘÍLOHY**

Přiložené DVD obsahuje následující soubory:

- BP-Zicha.pdf
- soubor s obrázky s technologií qWave
- soubor s obrázky s technologií WiDi
- soubor s obrázky s překrýváním kanálů